FIG. 1

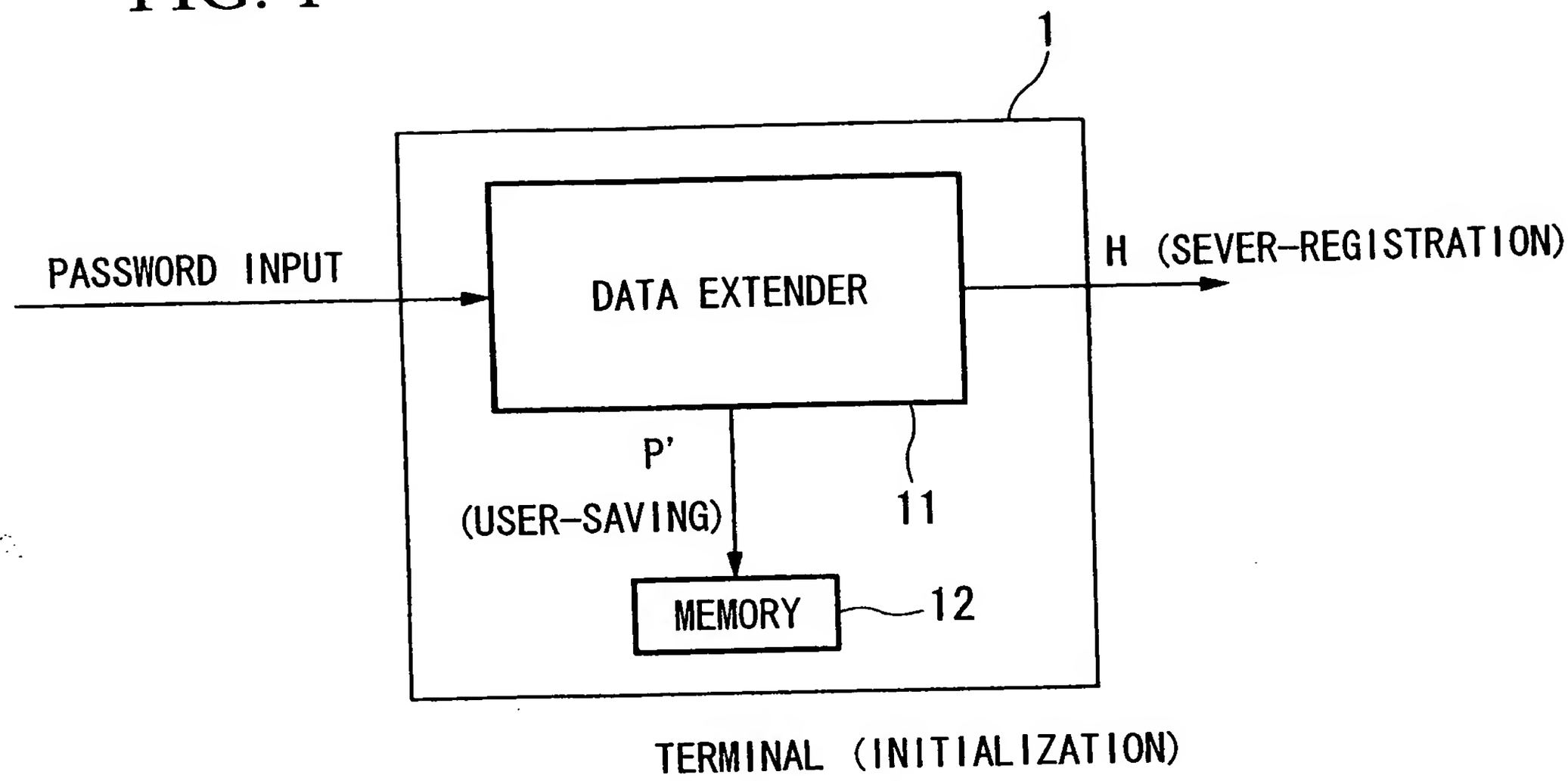

1
PASSWORD INPUT
DATA EXTENDER
H (SEVER-REGISTRATION)
P'
(USER-SAVING)
11
MEMORY
12
TERMINAL (INITIALIZATION)

FIG. 2

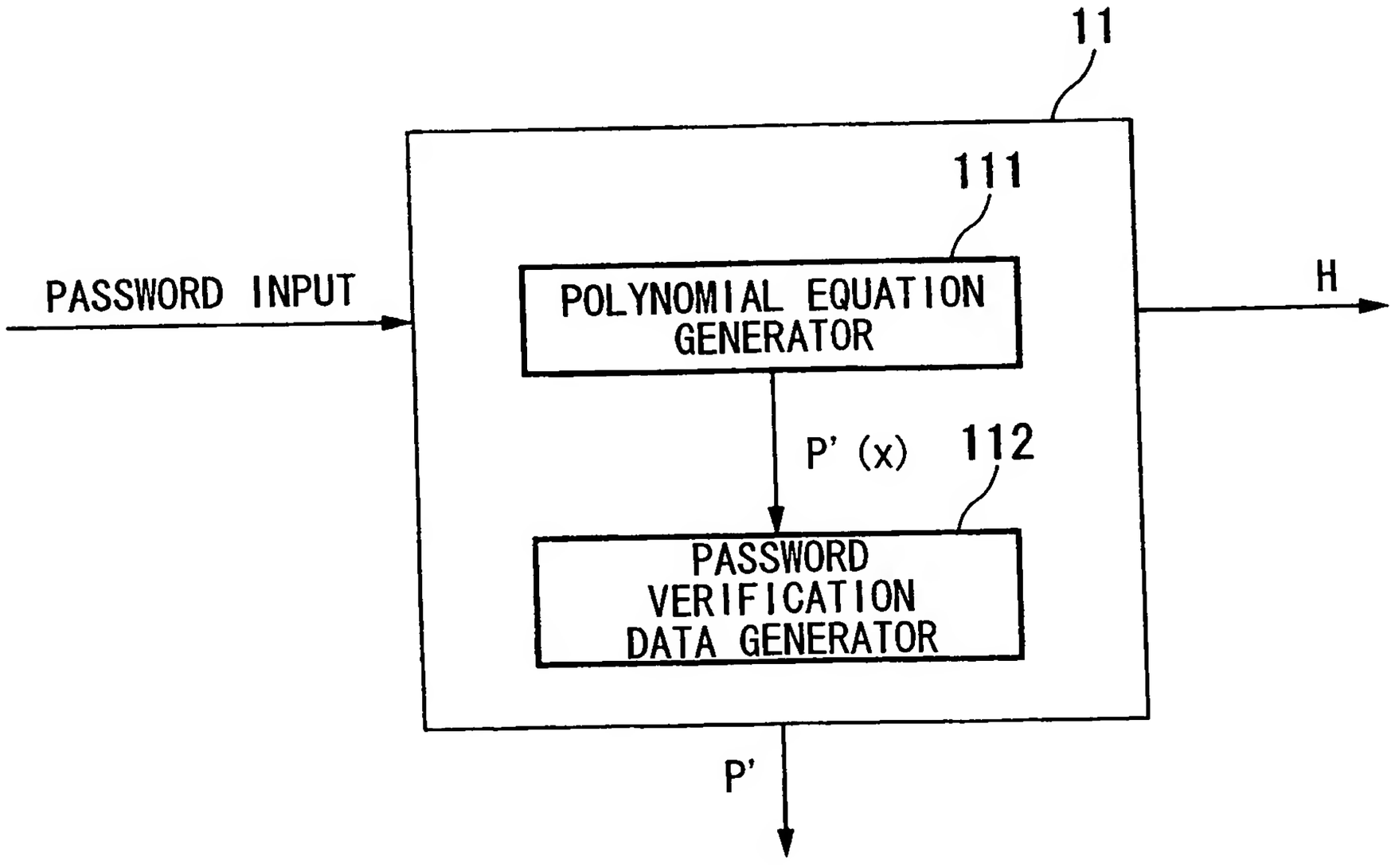

11
111
PASSWORD INPUT
POLYNOMIAL EQUATION GENERATOR
H
P' (x)
112
PASSWORD VERIFICATION DATA GENERATOR
P'

FIG. 3

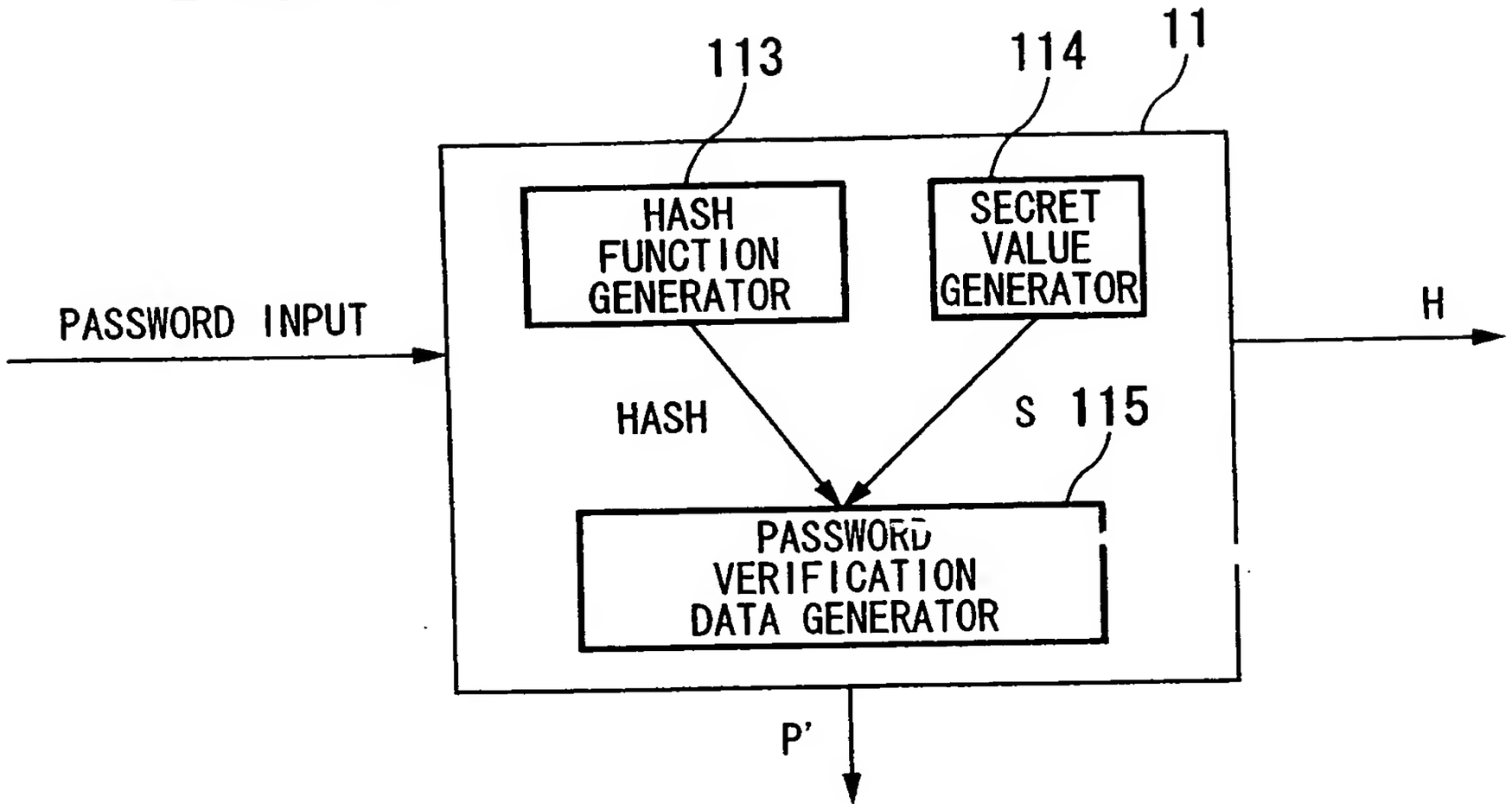

113
114
11
HASH FUNCTION GENERATOR
SECRET VALUE GENERATOR
PASSWORD INPUT
H
HASH
S
115
PASSWORD VERIFICATION DATA GENERATOR
P'

FIG. 4

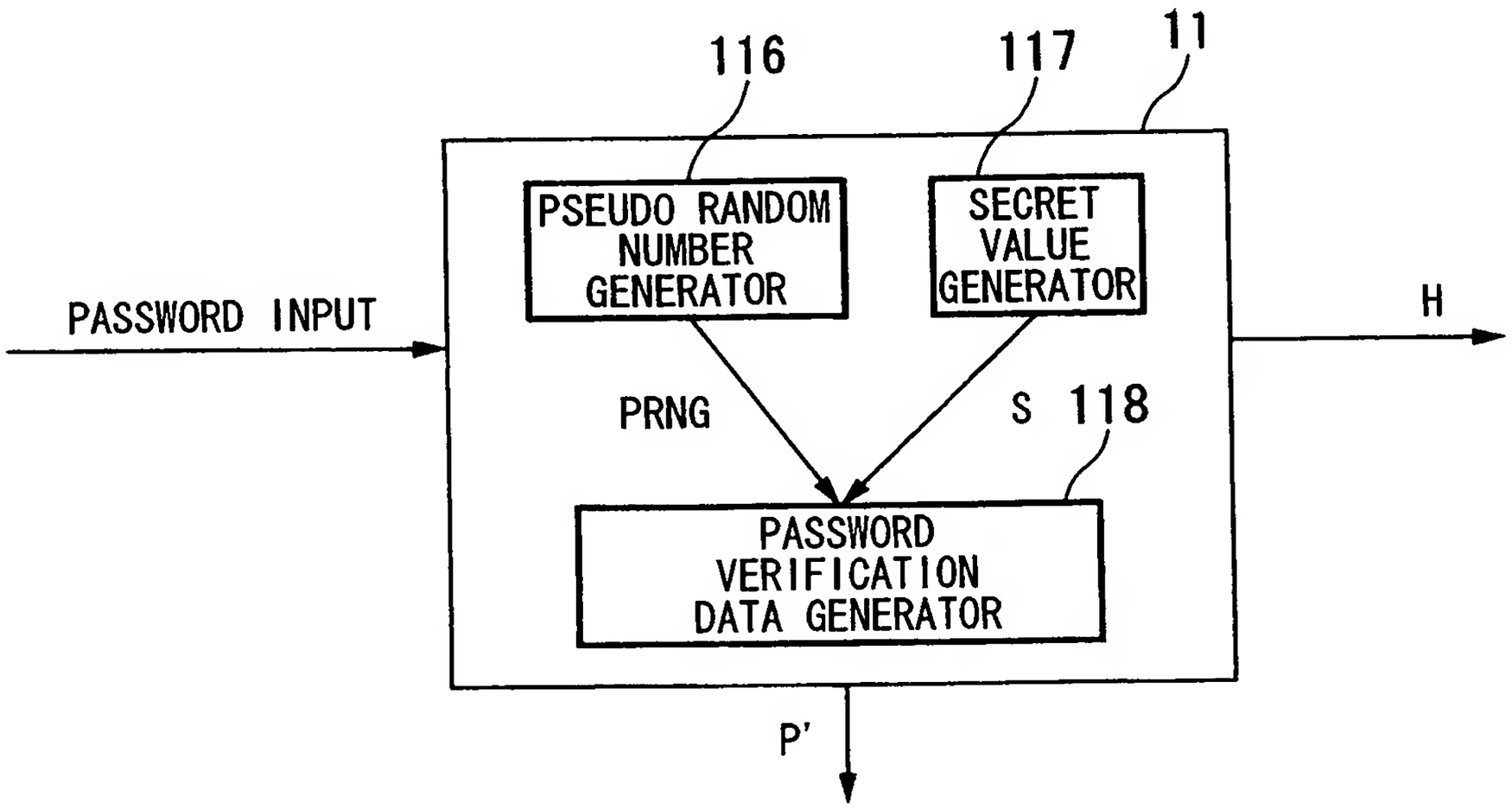

116
117
11
PSEUDO RANDOM NUMBER GENERATOR
SECRET VALUE GENERATOR
PASSWORD INPUT
H
PRNG
S
118
PASSWORD VERIFICATION DATA GENERATOR
P'

FIG. 5

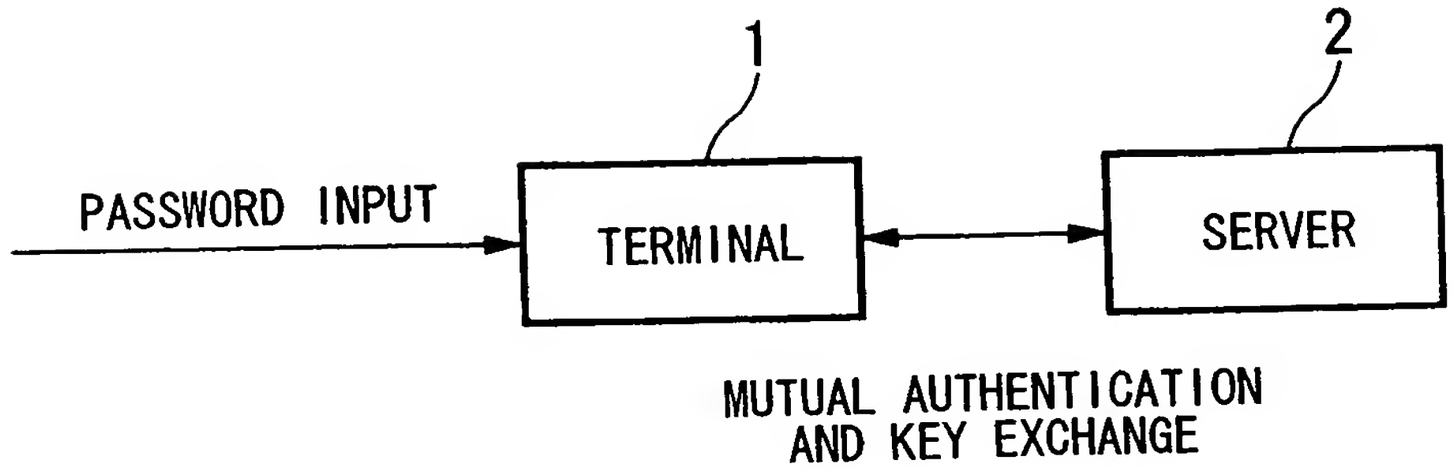

1
2
PASSWORD INPUT
TERMINAL
SERVER
MUTUAL AUTHENTICATION
AND KEY EXCHANGE

FIG. 6

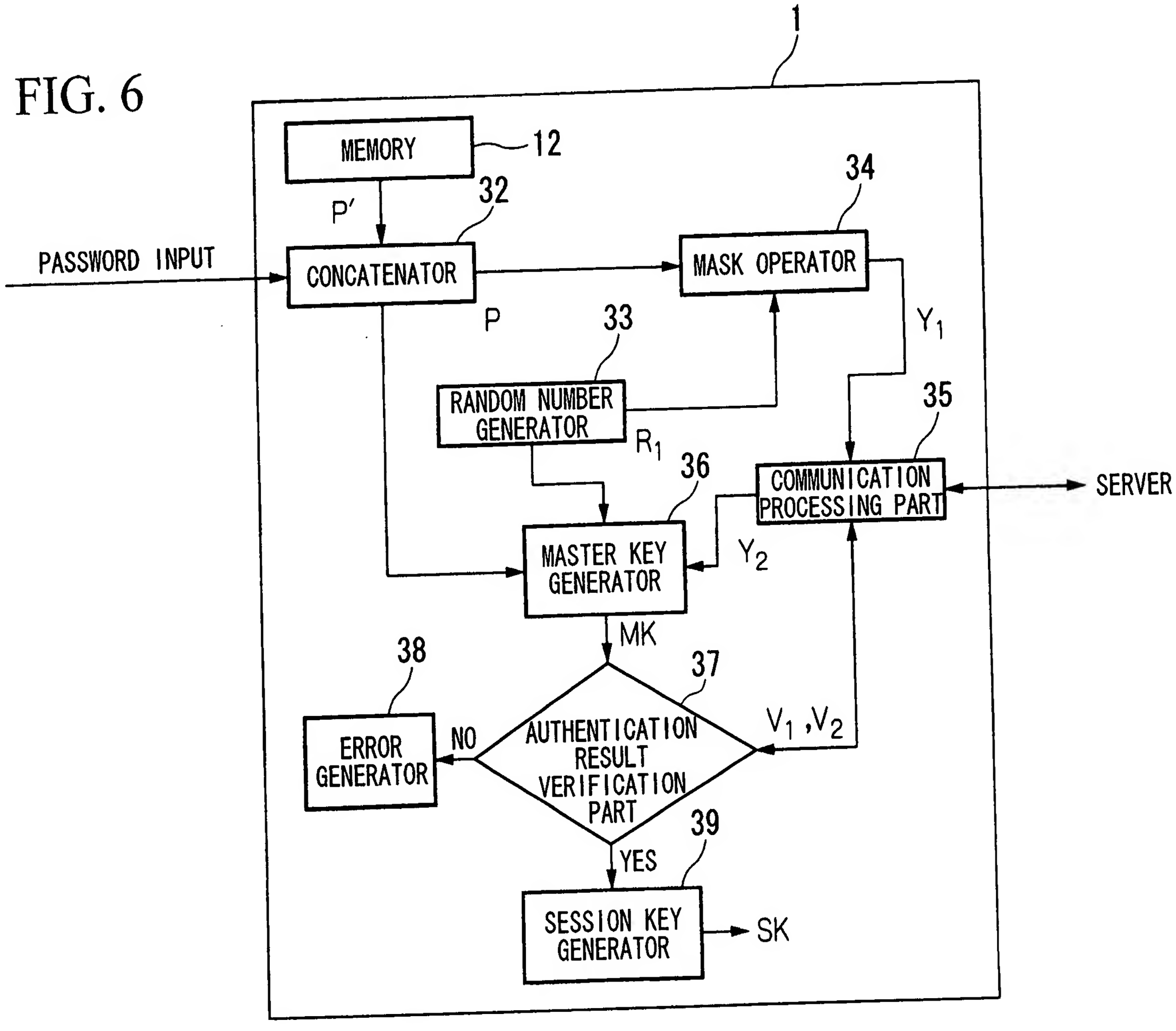

1
MEMORY
12
P'
32
34
PASSWORD INPUT
CONCATENATOR
MASK OPERATOR
P
33
Y_1
RANDOM NUMBER GENERATOR
R_1
35
36
COMMUNICATION PROCESSING PART
SERVER
MASTER KEY GENERATOR
Y_2
MK
38
37
ERROR GENERATOR
NO
AUTHENTICATION RESULT VERIFICATION PART
V_1 ,V_2
39
YES
SESSION KEY GENERATOR
SK

FIG. 7

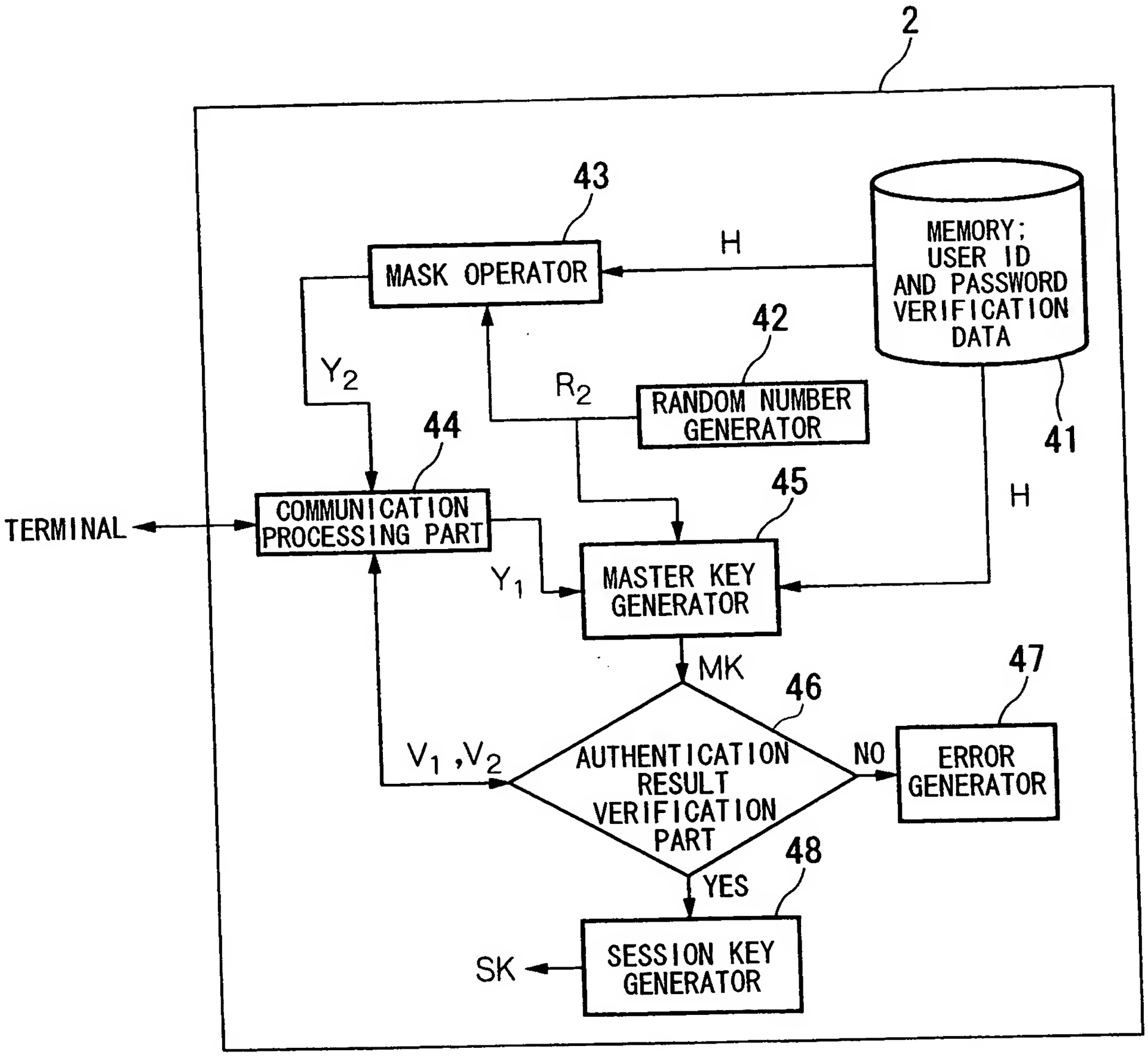

2
43
MASK OPERATOR
H
MEMORY;
USER ID
AND PASSWORD
VERIFICATION
DATA
42
Y_2
R_2
RANDOM NUMBER
GENERATOR
41
44
45
TERMINAL
COMMUNICATION
PROCESSING PART
H
Y_1
MASTER KEY
GENERATOR
MK
47
46
V_1 ,V_2
AUTHENTICATION
RESULT
VERIFICATION
PART
NO
ERROR
GENERATOR
48
YES
SK
SESSION KEY
GENERATOR

FIG. 8

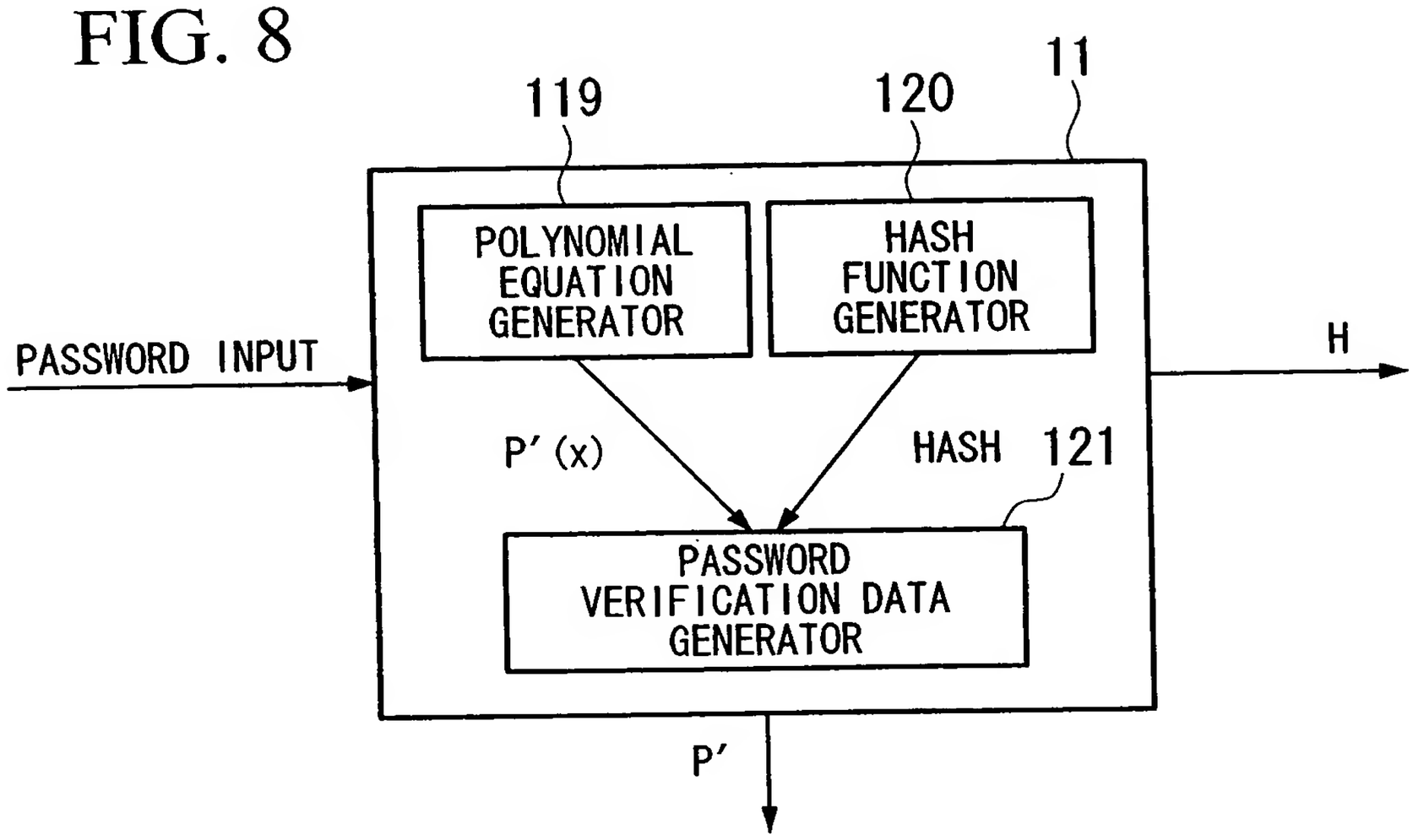

119
120
11
POLYNOMIAL EQUATION GENERATOR
HASH FUNCTION GENERATOR
PASSWORD INPUT
H
P′(x)
HASH
121
PASSWORD VERIFICATION DATA GENERATOR
P′

FIG. 9

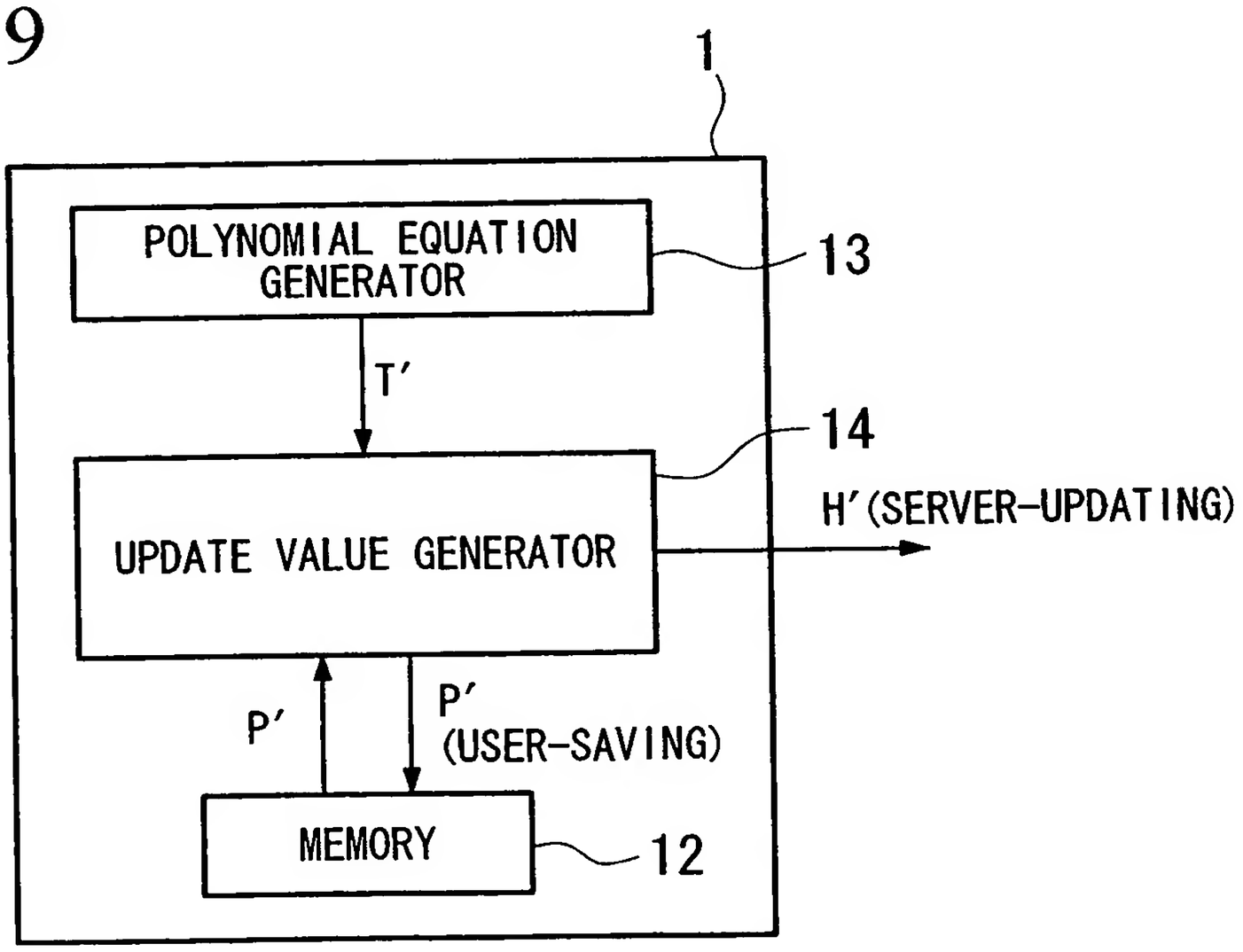

1
POLYNOMIAL EQUATION GENERATOR
13
T′
14
UPDATE VALUE GENERATOR
H′(SERVER-UPDATING)
P′
P′
(USER-SAVING)
MEMORY
12

FIG. 10

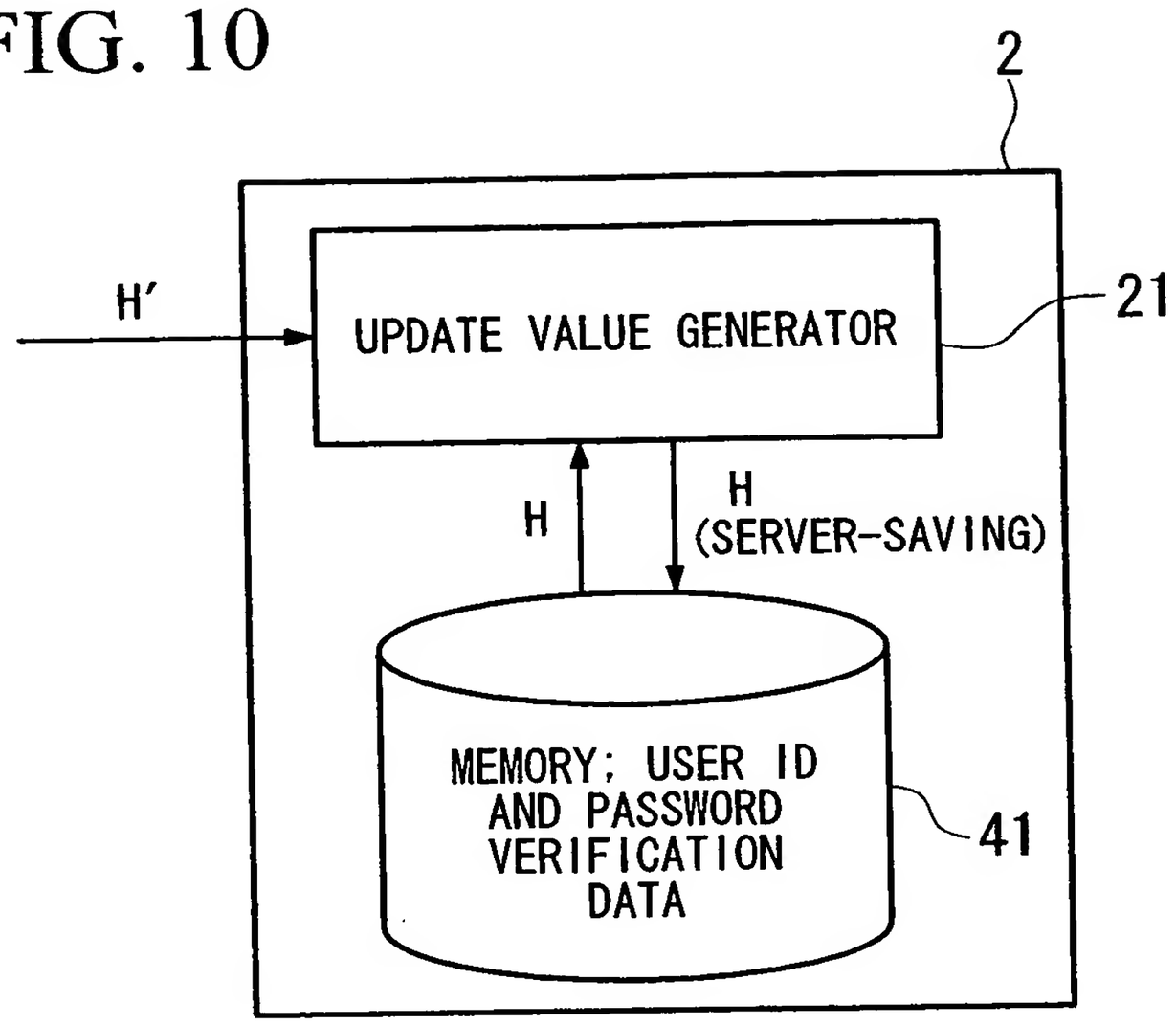

2
H′
UPDATE VALUE GENERATOR
21
H
H
(SERVER-SAVING)
MEMORY; USER ID
AND PASSWORD
VERIFICATION
DATA
41

FIG. 11

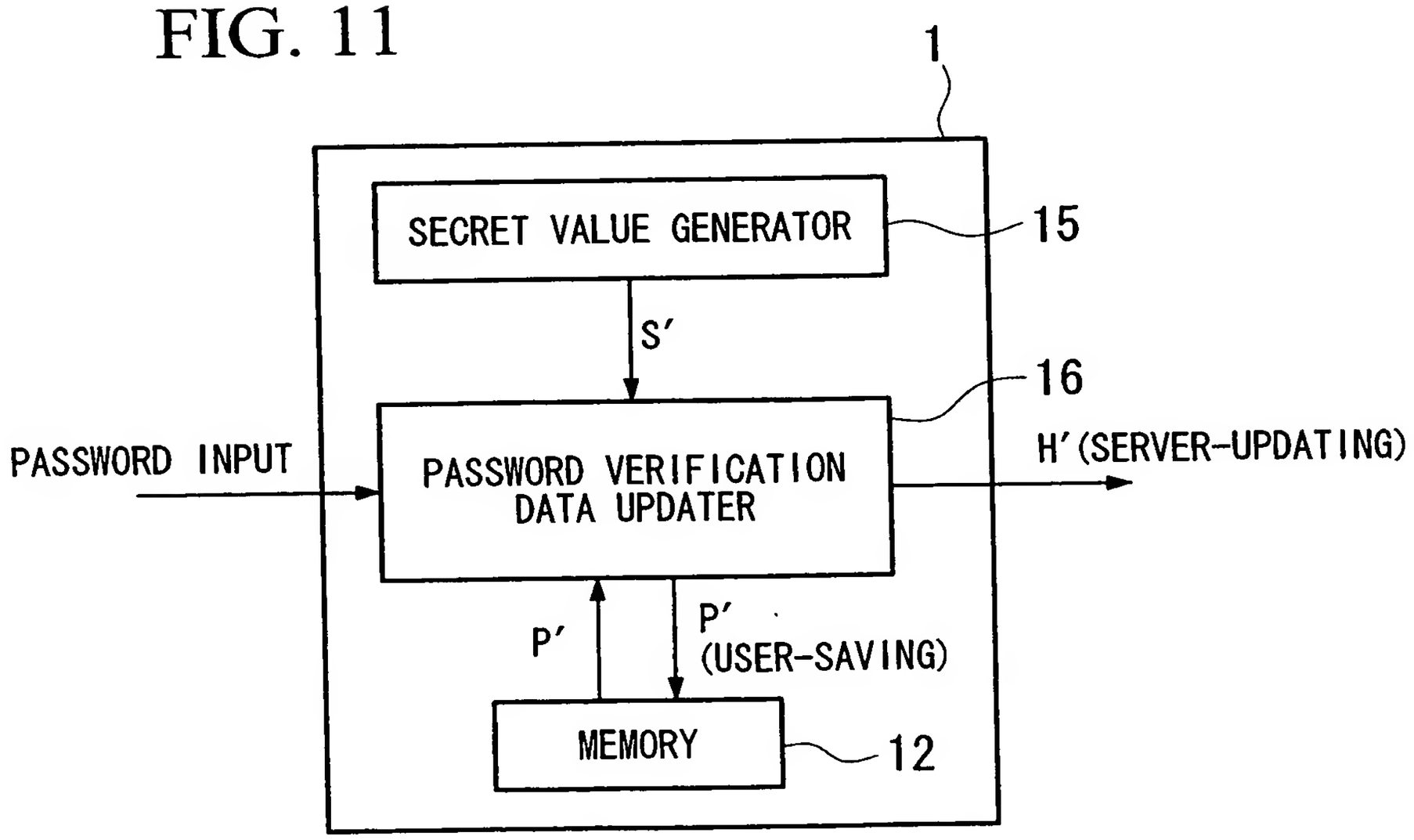

1
SECRET VALUE GENERATOR
15
S′
16
PASSWORD INPUT
PASSWORD VERIFICATION
DATA UPDATER
H′(SERVER-UPDATING)
P′
P′
(USER-SAVING)
MEMORY
12

FIG. 12

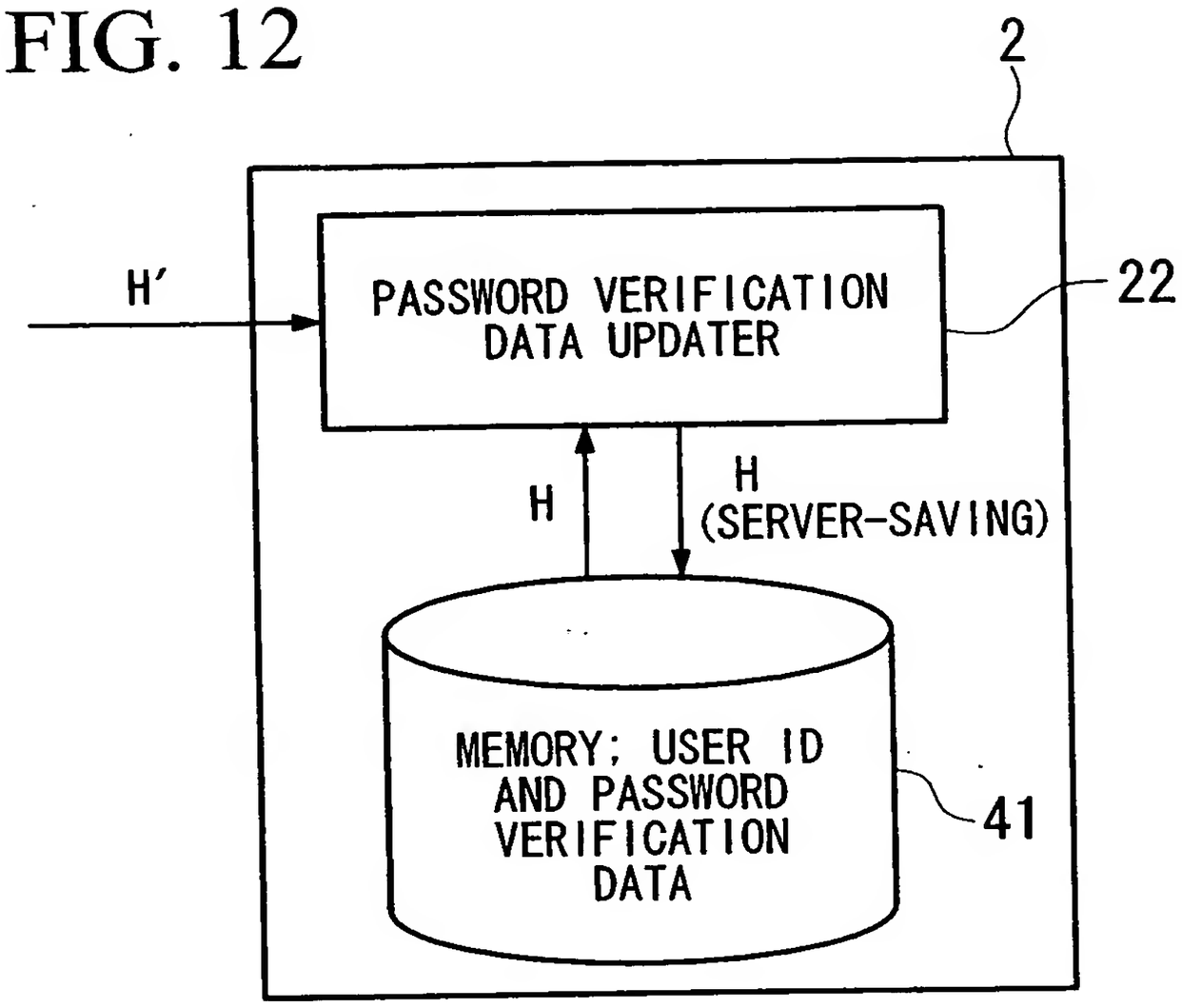

2
H'
PASSWORD VERIFICATION DATA UPDATER
22
H
H
(SERVER-SAVING)
MEMORY; USER ID AND PASSWORD VERIFICATION DATA
41

FIG. 13

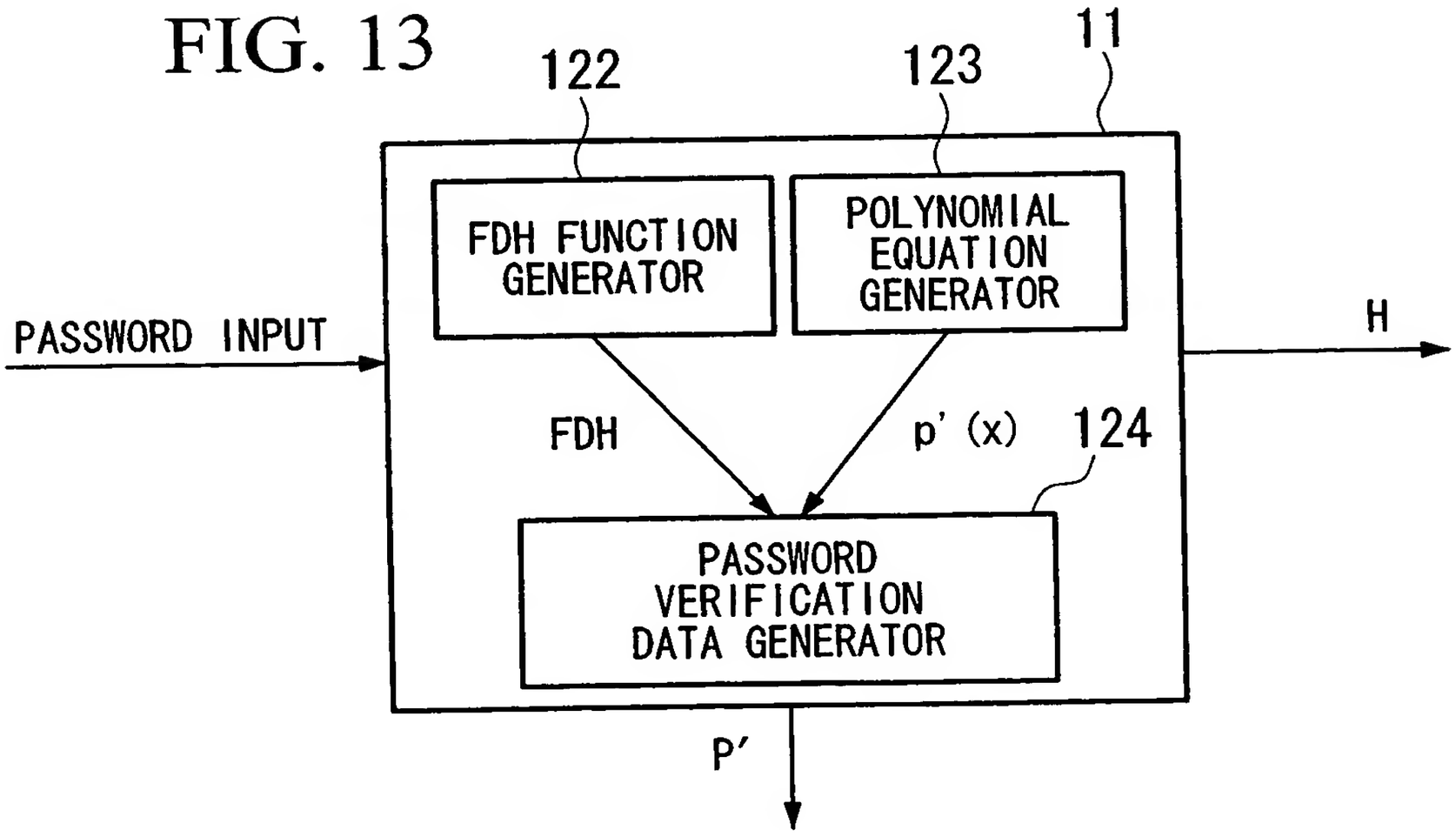

122
123
11
FDH FUNCTION GENERATOR
POLYNOMIAL EQUATION GENERATOR
PASSWORD INPUT
H
FDH
p' (x)
124
PASSWORD VERIFICATION DATA GENERATOR
P'

FIG. 14

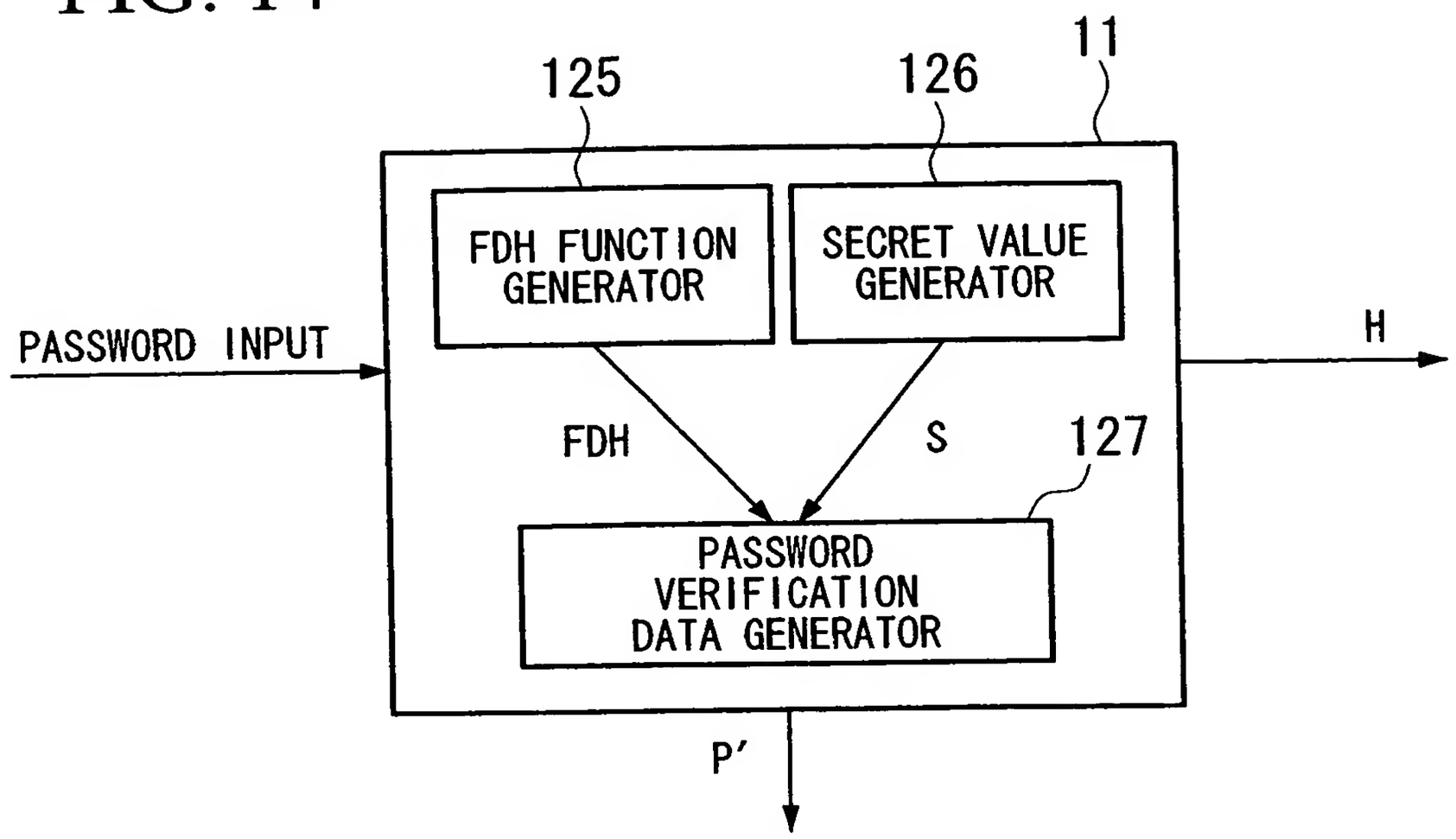

125
126
11
FDH FUNCTION GENERATOR
SECRET VALUE GENERATOR
PASSWORD INPUT
H
FDH
S
127
PASSWORD VERIFICATION DATA GENERATOR
P'

FIG. 15

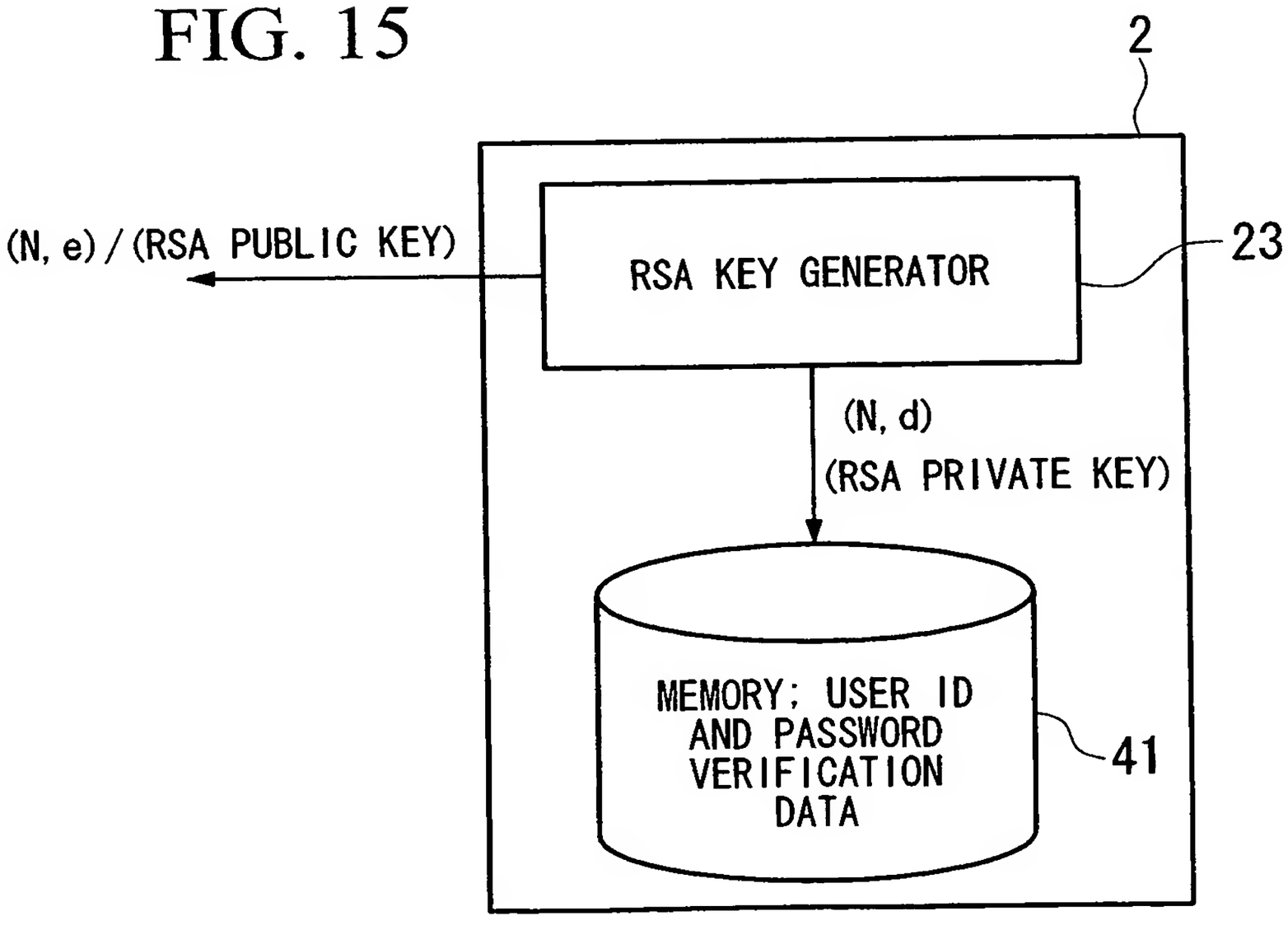

2
(N, e) / (RSA PUBLIC KEY)
RSA KEY GENERATOR
23
(N, d)
(RSA PRIVATE KEY)
MEMORY; USER ID AND PASSWORD VERIFICATION DATA
41

FIG. 16

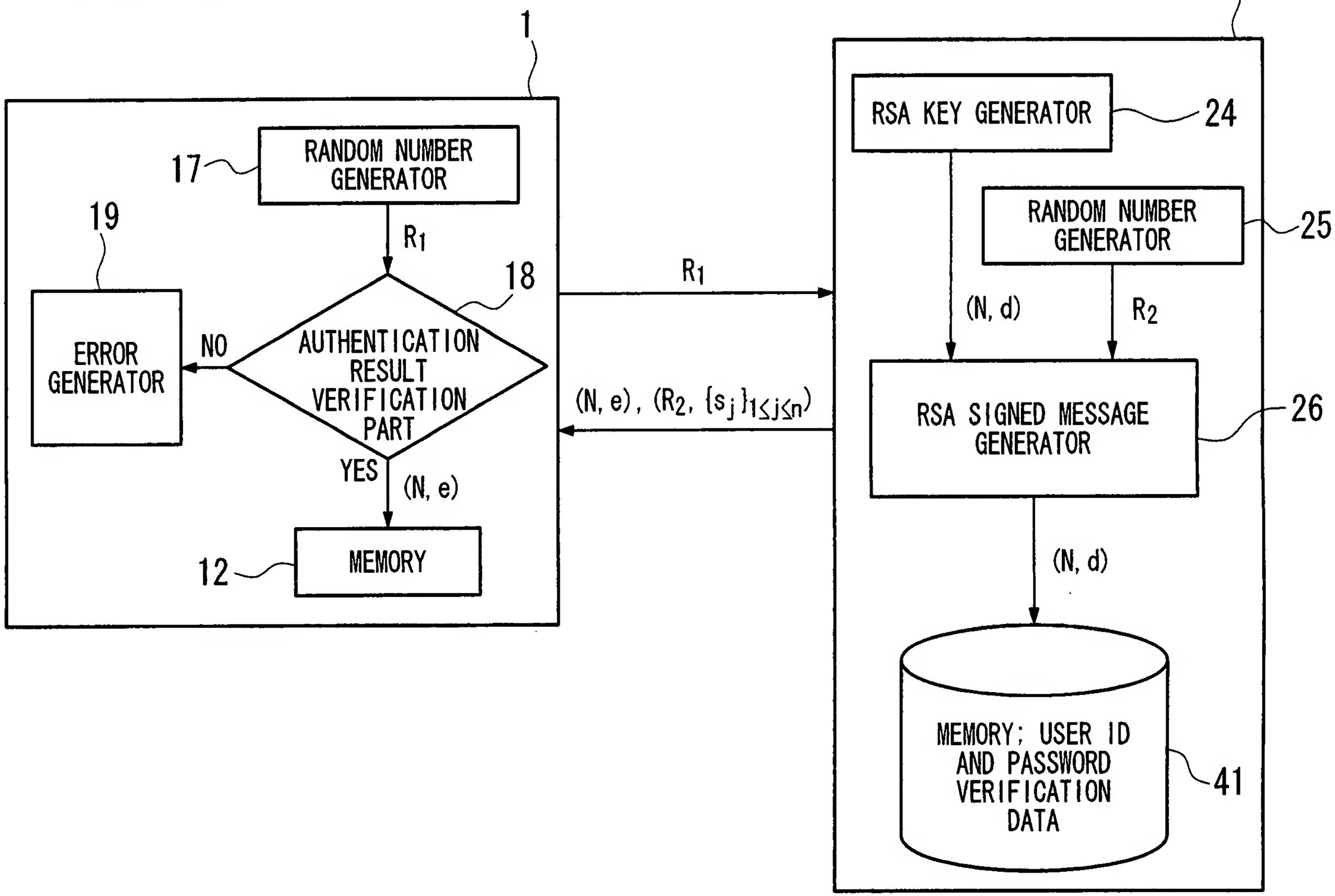

1
2
RANDOM NUMBER GENERATOR
17
19
R1
18
ERROR GENERATOR
NO
AUTHENTICATION RESULT VERIFICATION PART
YES
(N, e)
12
MEMORY
R1
(N, e), (R2, {sj}1≤j≤n)
RSA KEY GENERATOR
24
RANDOM NUMBER GENERATOR
25
(N, d)
R2
RSA SIGNED MESSAGE GENERATOR
26
(N, d)
MEMORY; USER ID AND PASSWORD VERIFICATION DATA
41

FIG. 17

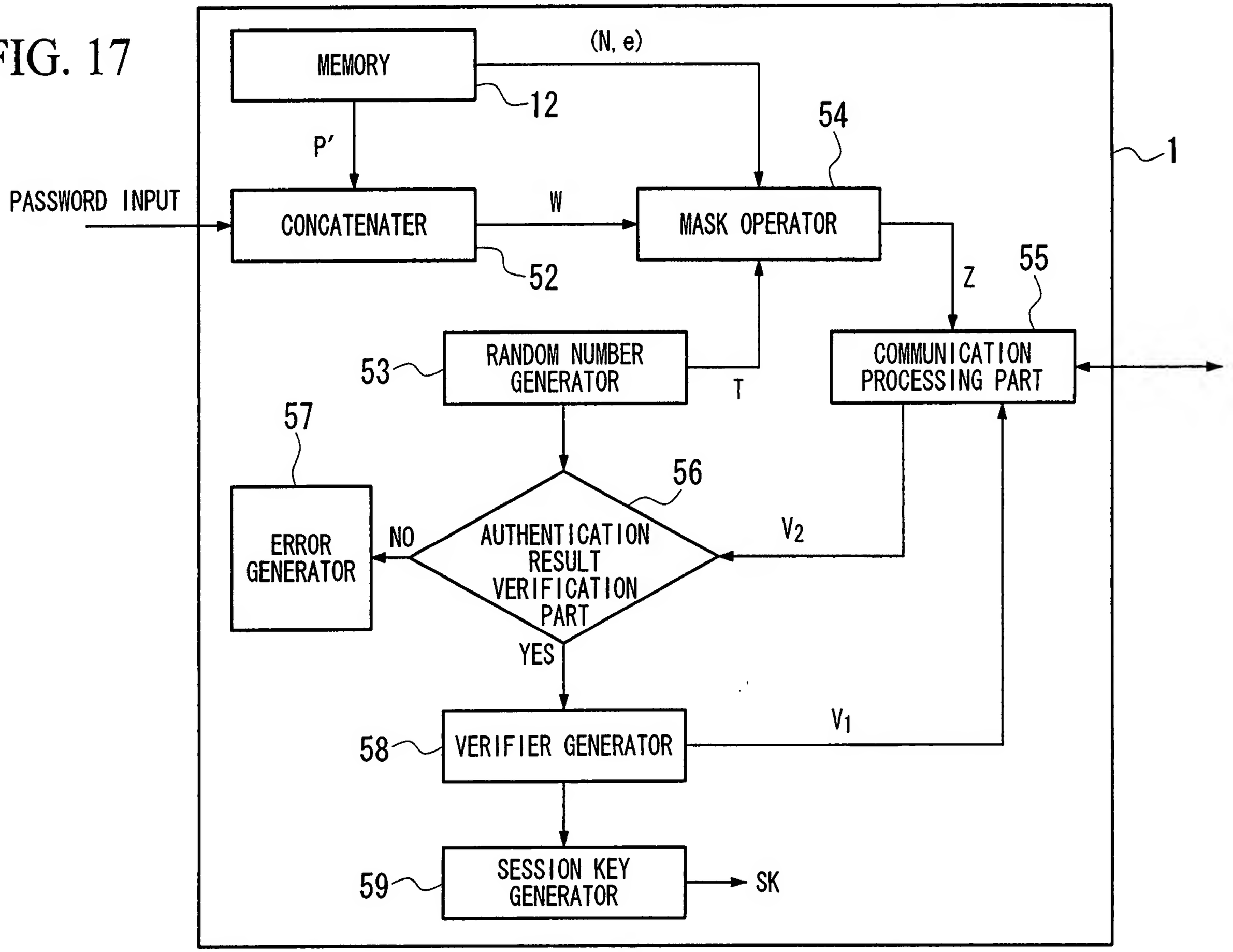

MEMORY
(N, e)
12
P′
54
1
PASSWORD INPUT
CONCATENATER
W
MASK OPERATOR
52
Z
55
RANDOM NUMBER GENERATOR
53
T
COMMUNICATION PROCESSING PART
57
56
ERROR GENERATOR
NO
AUTHENTICATION RESULT VERIFICATION PART
V2
YES
V1
58
VERIFIER GENERATOR
59
SESSION KEY GENERATOR
SK

FIG. 18

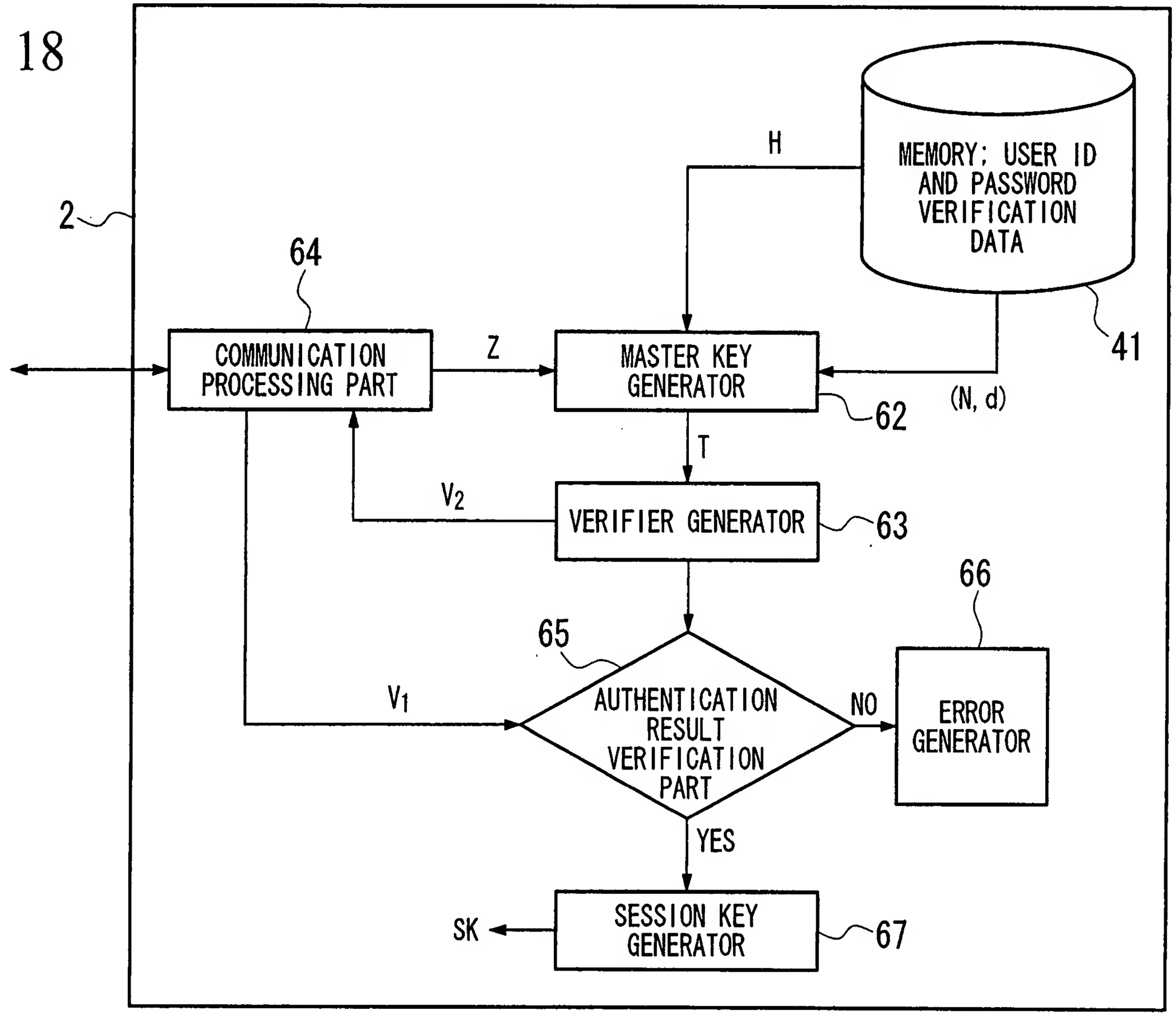

2
64
COMMUNICATION PROCESSING PART
Z
MASTER KEY GENERATOR
62
H
MEMORY: USER ID AND PASSWORD VERIFICATION DATA
41
(N, d)
T
V_2
VERIFIER GENERATOR
63
66
65
V_1
AUTHENTICATION RESULT VERIFICATION PART
NO
ERROR GENERATOR
YES
SK
SESSION KEY GENERATOR
67

FIG. 19

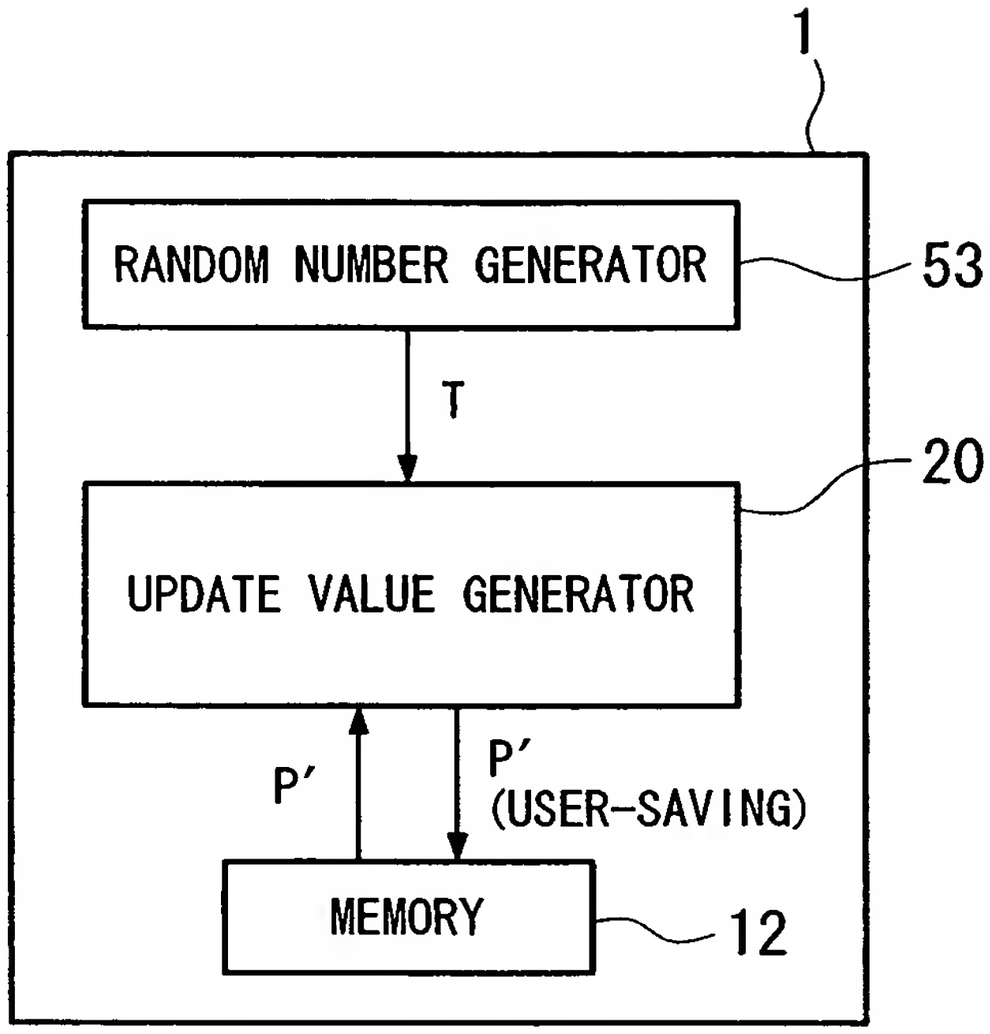

1
RANDOM NUMBER GENERATOR
53
T
20
UPDATE VALUE GENERATOR
P′
P′
(USER-SAVING)
MEMORY
12

FIG. 20

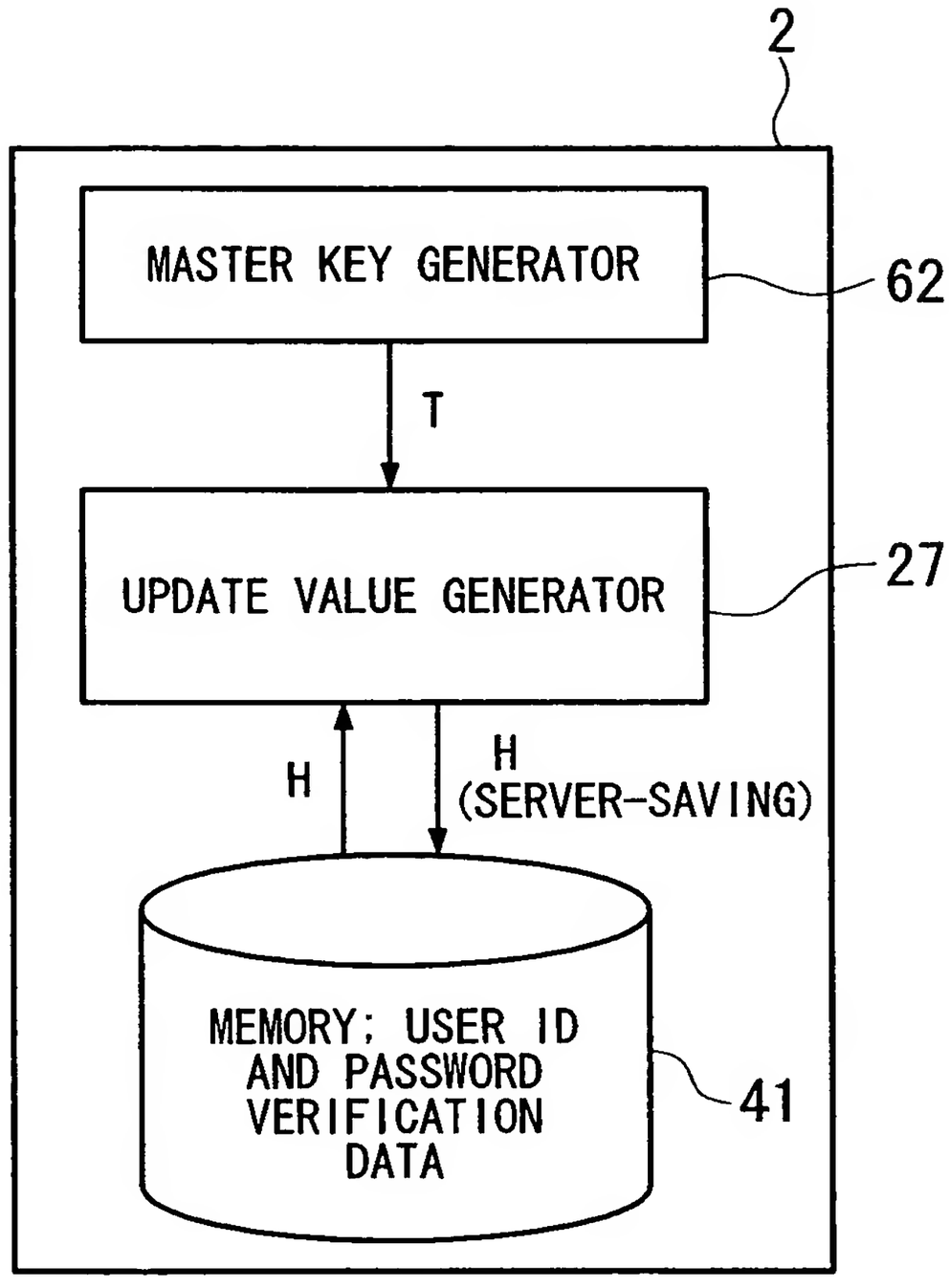

2
MASTER KEY GENERATOR
62
T
UPDATE VALUE GENERATOR
27
H
H
(SERVER-SAVING)
MEMORY; USER ID
AND PASSWORD
VERIFICATION
DATA
41

FIG. 21

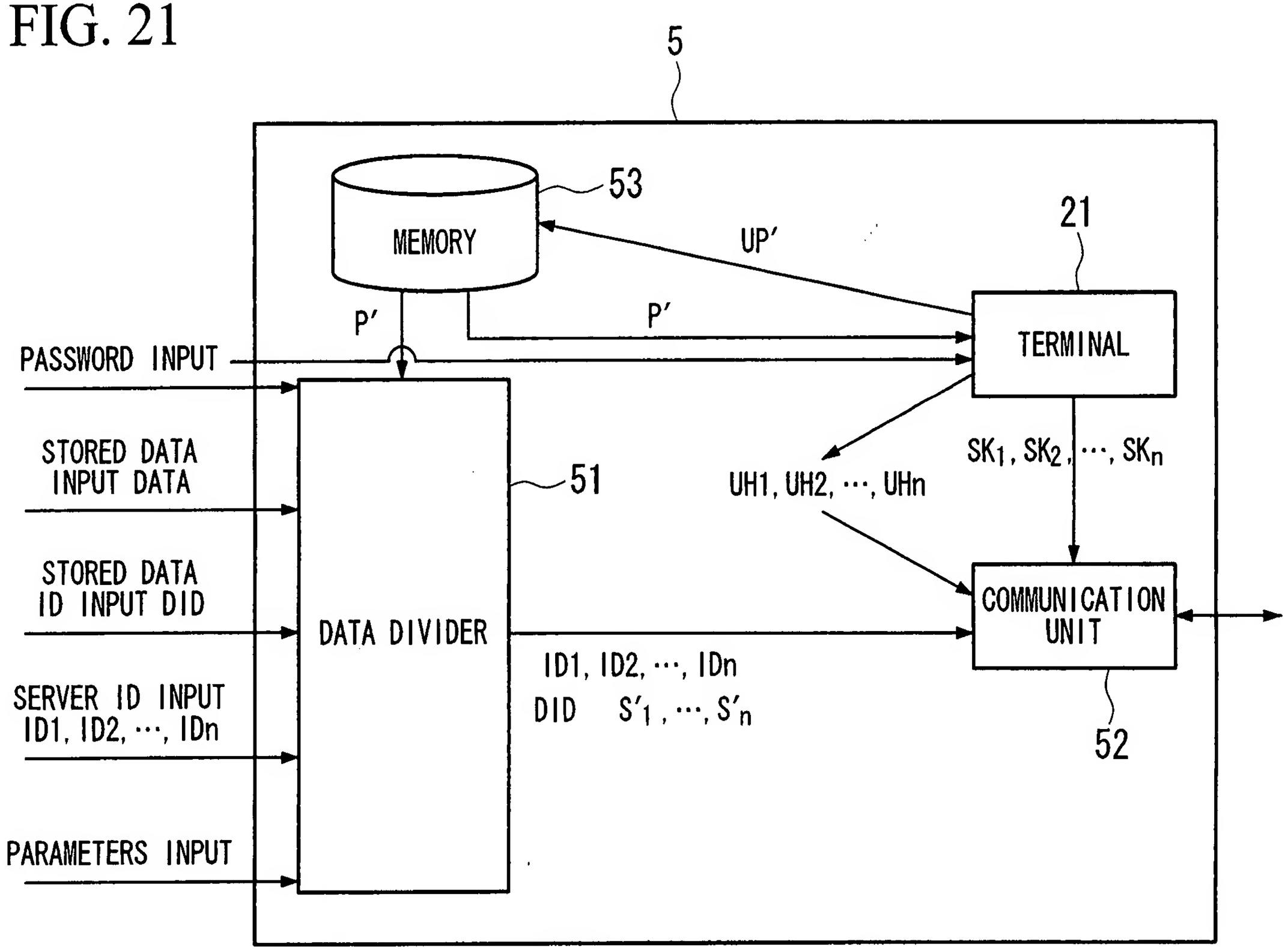

5
MEMORY
53
UP'
21
P'
P'
TERMINAL
PASSWORD INPUT
STORED DATA
INPUT DATA
51
UH1, UH2, ···, UHn
SK1, SK2, ···, SKn
STORED DATA
ID INPUT DID
DATA DIVIDER
COMMUNICATION
UNIT
ID1, ID2, ···, IDn
DID S'1, ···, S'n
SERVER ID INPUT
ID1, ID2, ···, IDn
52
PARAMETERS INPUT

FIG. 22

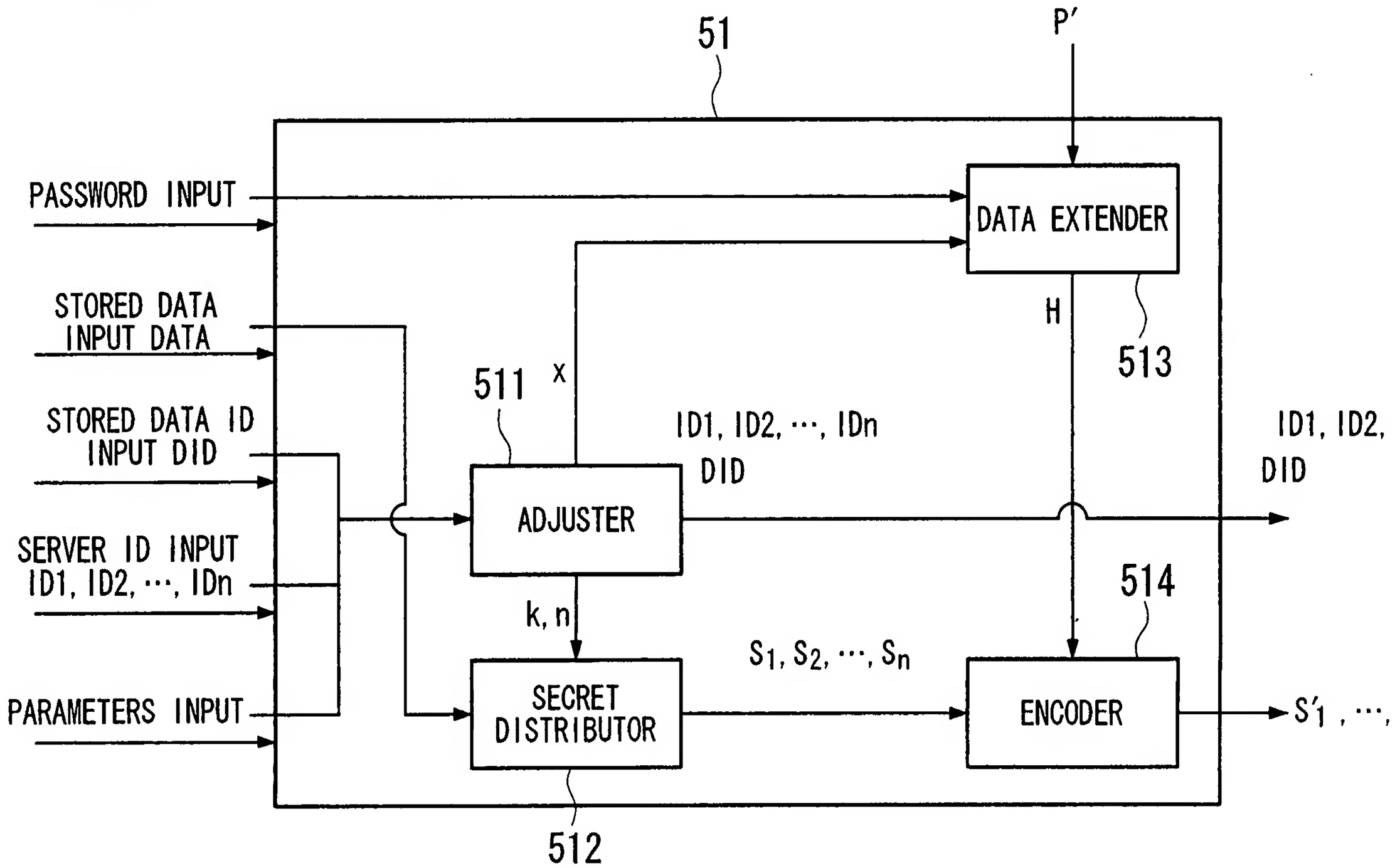

51
P'
PASSWORD INPUT
DATA EXTENDER
STORED DATA
INPUT DATA
H
513
511
X
STORED DATA ID
INPUT DID
ID1, ID2, ···, IDn
DID
ID1, ID2,
DID
ADJUSTER
SERVER ID INPUT
ID1, ID2, ···, IDn
514
k, n
$S_1, S_2, \cdots, S_n$
PARAMETERS INPUT
SECRET
DISTRIBUTOR
ENCODER
$S'_1, \cdots,$
512

FIG. 23

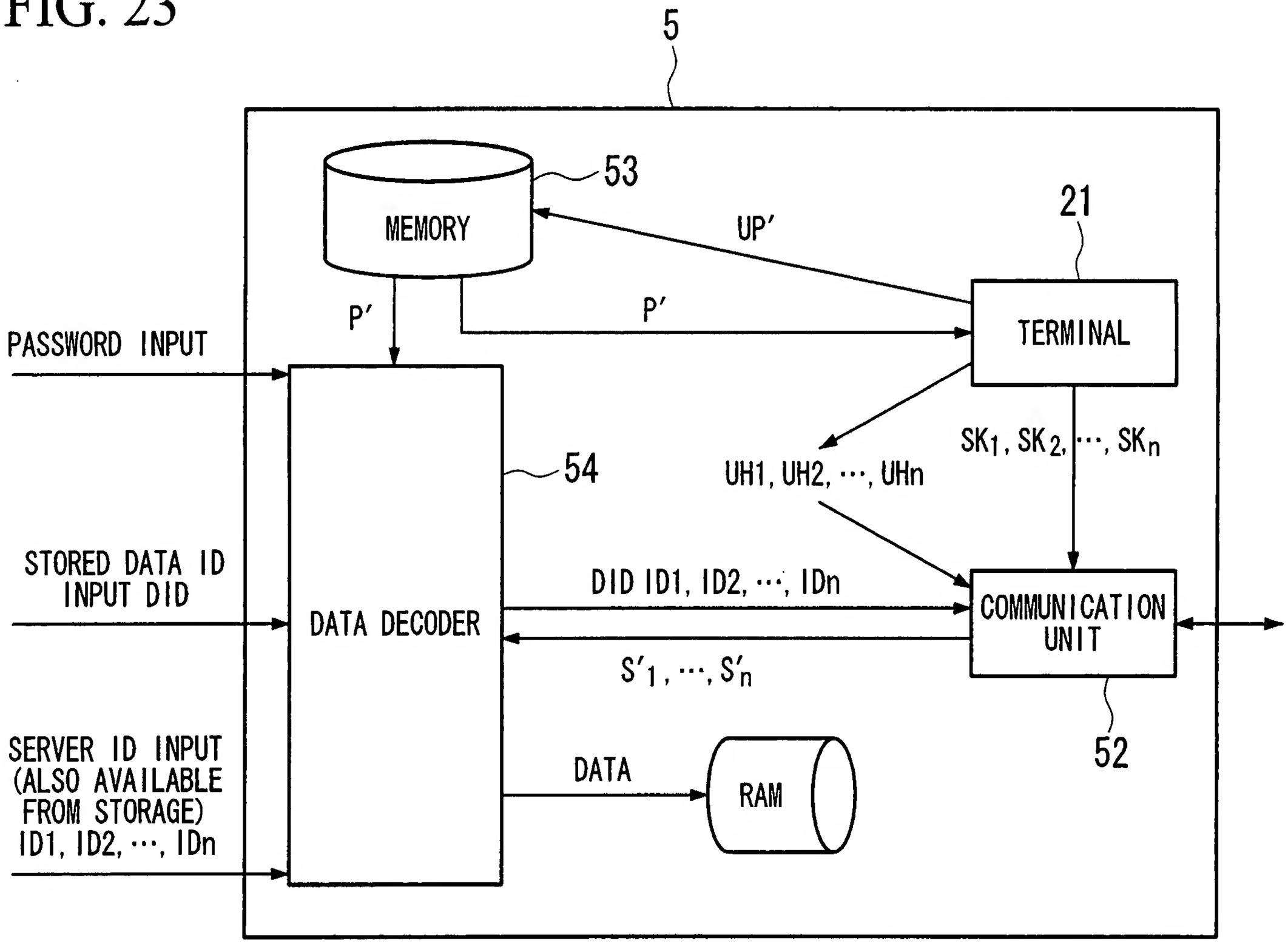

5
53
MEMORY
UP'
21
P'
P'
TERMINAL
PASSWORD INPUT
54
UH1, UH2, ···, UHn
SK1, SK2, ···, SKn
STORED DATA ID
INPUT DID
DID ID1, ID2, ···, IDn
DATA DECODER
COMMUNICATION
UNIT
S'1, ···, S'n
52
SERVER ID INPUT
(ALSO AVAILABLE
FROM STORAGE)
ID1, ID2, ···, IDn
DATA
RAM

FIG. 24

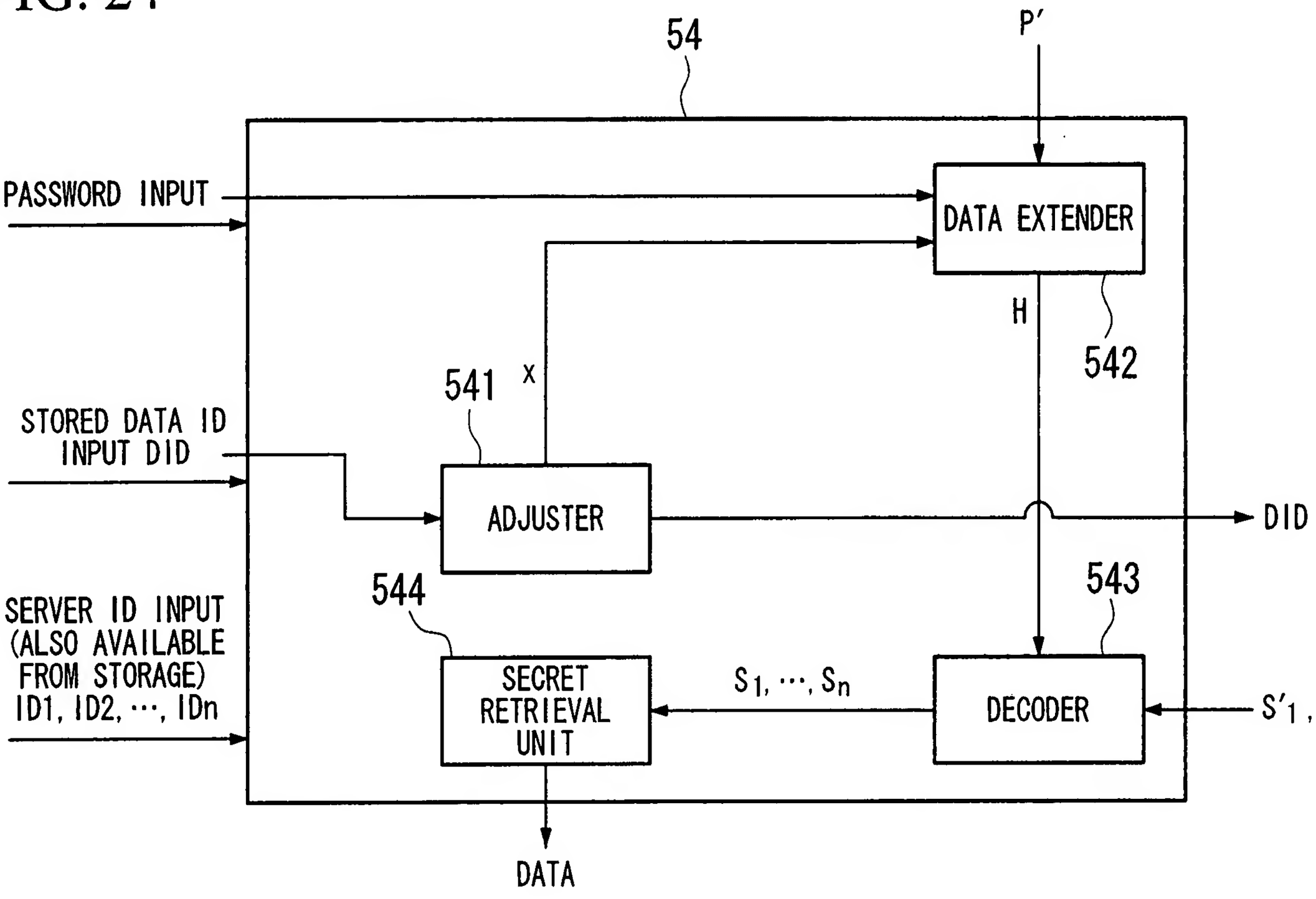

54
P′
PASSWORD INPUT
DATA EXTENDER
H
542
541
X
STORED DATA ID
INPUT DID
ADJUSTER
DID
544
543
SERVER ID INPUT
(ALSO AVAILABLE
FROM STORAGE)
ID1, ID2, ···, IDn
SECRET
RETRIEVAL
UNIT
S1, ···, Sn
DECODER
S′1,
DATA

FIG. 25

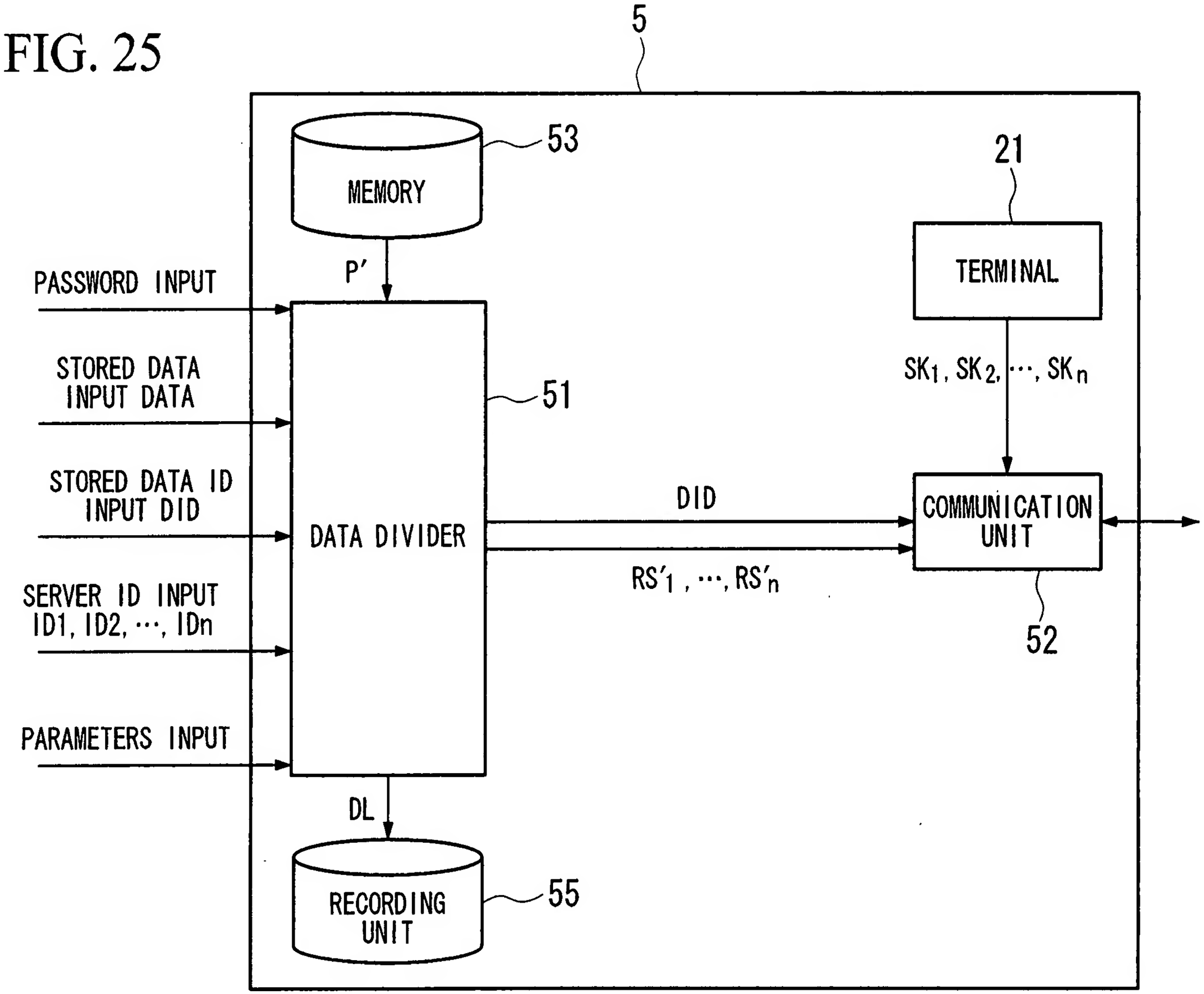

5
MEMORY
53
21
TERMINAL
P'
PASSWORD INPUT
STORED DATA
INPUT DATA
51
$SK_1, SK_2, \cdots, SK_n$
STORED DATA ID
INPUT DID
DATA DIVIDER
DID
COMMUNICATION
UNIT
$RS'_1, \cdots, RS'_n$
SERVER ID INPUT
ID1, ID2, ···, IDn
52
PARAMETERS INPUT
DL
RECORDING
UNIT
55

FIG. 26

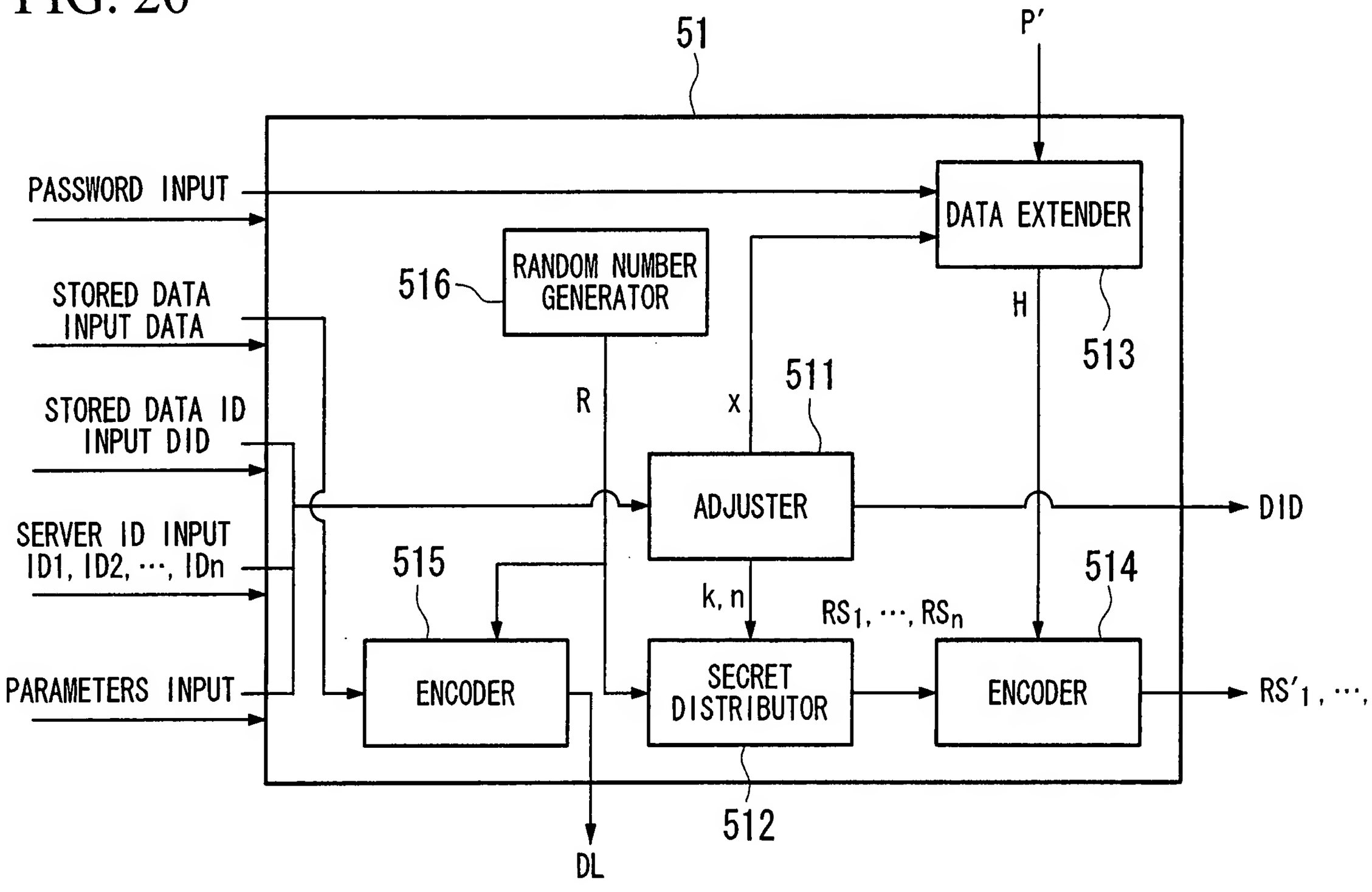

51
P'
PASSWORD INPUT
DATA EXTENDER
516
RANDOM NUMBER GENERATOR
STORED DATA INPUT DATA
H
513
R
X
511
STORED DATA ID INPUT DID
ADJUSTER
DID
SERVER ID INPUT ID1, ID2, ···, IDn
515
514
k, n
RS1, ···, RSn
PARAMETERS INPUT
ENCODER
SECRET DISTRIBUTOR
ENCODER
RS'1, ···,
512
DL

FIG. 27

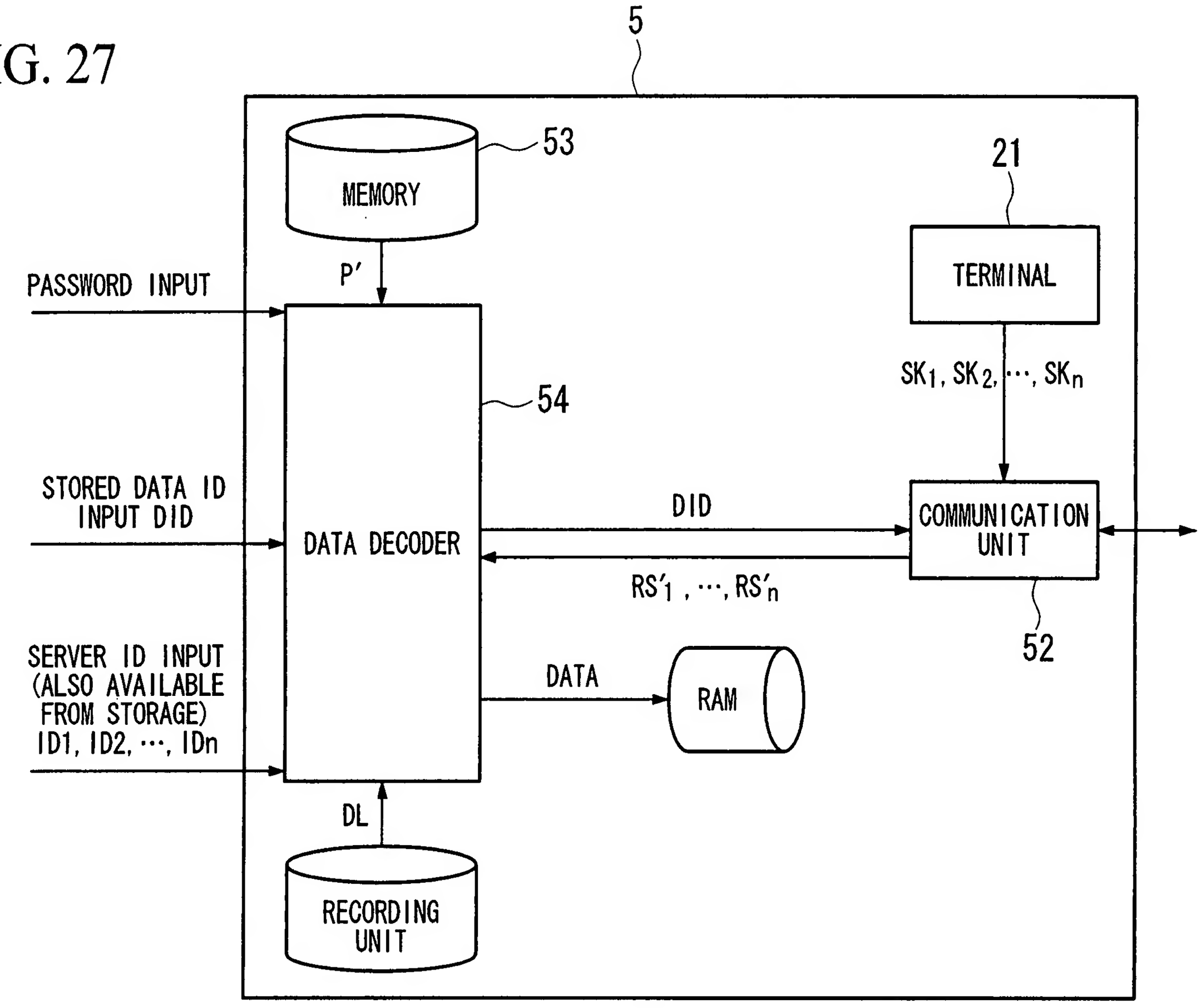
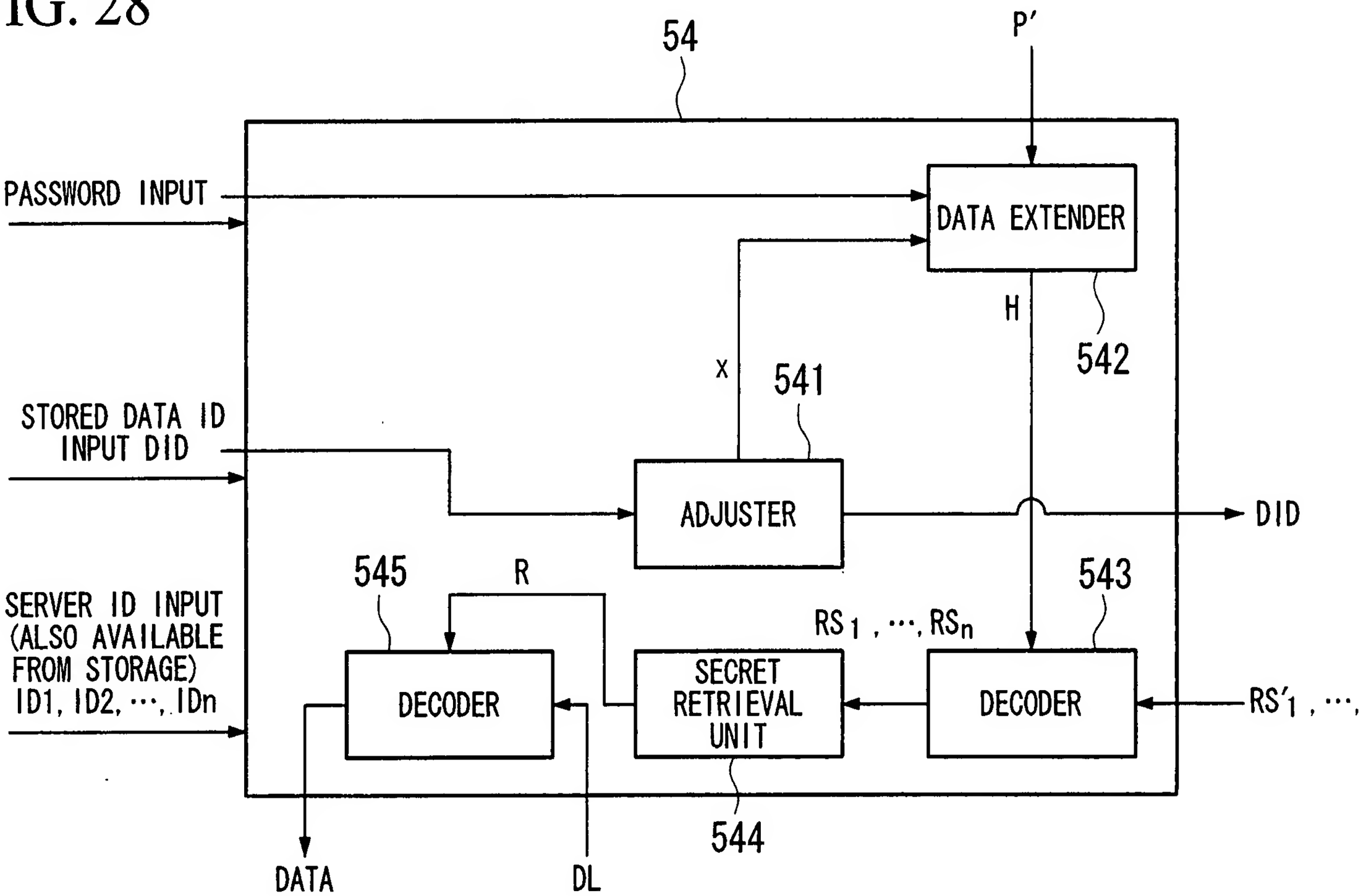

5
53
MEMORY
21
TERMINAL
P'
PASSWORD INPUT
54
$SK_1, SK_2, \cdots, SK_n$
STORED DATA ID
INPUT DID
DATA DECODER
DID
COMMUNICATION
UNIT
$RS'_1, \cdots, RS'_n$
52
SERVER ID INPUT
(ALSO AVAILABLE
FROM STORAGE)
ID1, ID2, ···, IDn
DATA
RAM
DL
RECORDING
UNIT

FIG. 28


54
P'
PASSWORD INPUT
DATA EXTENDER
H
542
X
541
STORED DATA ID
INPUT DID
ADJUSTER
DID
545
R
543
SERVER ID INPUT
(ALSO AVAILABLE
FROM STORAGE)
ID1, ID2, ···, IDn
RS1, ···, RSn
DECODER
SECRET
RETRIEVAL
UNIT
DECODER
RS'1, ···,
544
DATA
DL